



### Certification of Translation

I, Robin Holding, having an office at 948 15th Street, #4, Santa Monica, CA 90403 USA, hereby state that I am well acquainted with both the English and French languages and that to the best of my knowledge and ability, the appended document is a true and faithful translation of

**a certified copy of French Patent Application No. 0007978, in the name of BULL CP8, filed on June 22, 2000.**

I further declare that the above statement is true; and further, that this statement is made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent resulting therefrom.

January 9, 2006

Date

*Robin Holding*  
Robin Holding

**THIS PAGE BLANK (USPTO)**



BEST AVAILABLE COPY

---

# BREVET D'INVENTION

---

**CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION****COPIE OFFICIELLE**

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **05 DEC. 2005**

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

A handwritten signature in black ink, appearing to read 'M+Planche', enclosed within a large, loopy oval stroke.

Martine PLANCHE

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint-Petersbourg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
[www.inpi.fr](http://www.inpi.fr)



**THIS PAGE BLANK (USPTO)**

<b>REMISE DES PIÈCES</b> DATE <b>22 JUIN 2000</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI <b>0007978</b> DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI <b>22 JUIN 2000</b>		<b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE          À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</b>  <b>BULL S.A.</b> <b>CORLU</b> Bernard - PC/58D20 68, route de Versailles  <b>78434 LOUVECIENNES Cedex</b>	
<b>Vos références pour ce dossier</b> (facultatif) <b>FR 3882/BC</b>			
<b>Confirmation d'un dépôt par télécopie</b>		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
<b>2 NATURE DE LA DEMANDE</b>		<b>Cochez l'une des 4 cases suivantes</b>	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N° _____ Date : ____ / ____ / ____ N° _____ Date : ____ / ____ / ____	
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N° _____ Date : ____ / ____ / ____	
<b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b>  <b>PROCÉDÉ POUR LE TRAITEMENT ET LA TRANSMISSION DE DONNÉES NUMÉRIQUES SUR UN          RÉSEAU DE TÉLÉPHONIE MOBILE, NOTAMMENT À LA NORME "GSM", ET SYSTÈME          EMBARQUÉ À PUCE ÉLECTRONIQUE.</b>			
<b>4 DÉCLARATION DE PRIORITÉ          OU REQUÊTE DU BÉNÉFICE DE          LA DATE DE DÉPÔT D'UNE          DEMANDE ANTÉRIEURE FRANÇAISE</b>		Pays ou organisation _____ N° _____ Date : ____ / ____ / ____ Pays ou organisation _____ N° _____ Date : ____ / ____ / ____ Pays ou organisation _____ N° _____ Date : ____ / ____ / ____ <input type="checkbox"/> <b>S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</b>	
<b>5 DEMANDEUR</b>		<input type="checkbox"/> <b>S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</b>	
Nom ou dénomination sociale		<b>BULL CP8</b>	
Prénoms			
Forme juridique		<b>Société Anonyme</b>	
N° SIREN		<b>3 2 9 5 5 6 1 4 6</b>	
Code APE-NAF		<b>B 3 2 1</b>	
Adresse	Rue	<b>BP 45 - 68, route de Versailles</b>	
	Code postal et ville	<b>78430</b>	<b>LOUVECIENNES</b>
Pays		<b>France</b>	
Nationalité		<b>Française</b>	
N° de téléphone (facultatif)		<b>01.39.66.61.76</b>	
N° de télécopie (facultatif)		<b>01.39.66.61.73</b>	
Adresse électronique (facultatif)		<b>BERNARD.CORLU@BULL.NET</b>	

Réservé à l'INPI

REMISE DES PIÈCES

DATE

22 JUIN 2000

LIEU

75 INPI PARIS

N° D'ENREGISTREMENT

NATIONAL ATTRIBUÉ PAR L'INPI

0007978

DB 540 W / 260899

<b>Vos références pour ce dossier :</b> (facultatif)		FR 3882/BC	
<b>6 MANDATAIRE</b>			
Nom		CORLU	
Prénom		Bernard	
Cabinet ou Société		BULL S.A.	
N° de pouvoir permanent et/ou de lien contractuel		PG 4280	
Adresse	Rue	68, route de Versailles / PC 58D20	
	Code postal et ville	78434 LOUVECIENNES CEDEX	
N° de téléphone (facultatif)		01.39.66.61.76	
N° de télécopie (facultatif)		01.39.66.61.73	
Adresse électronique (facultatif)		BERNARD.CORLU@BULL.NET	
<b>7 INVENTEUR (S)</b>			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
<b>8 RAPPORT DE RECHERCHE</b>		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		<b>Paiement en trois versements, uniquement pour les personnes physiques</b> <input type="checkbox"/> Oui <input type="checkbox"/> Non	
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		<b>Uniquement pour les personnes physiques</b> <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		0	
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire)		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>	
CORLU Bernard (Mandataire)		H. ADAO	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° ... 1 / 1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		FR 3882/BC	
N° D'ENREGISTREMENT NATIONAL		000 7978	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
PROCÉDÉ POUR LE TRAITEMENT ET LA TRANSMISSION DE DONNÉES NUMÉRIQUES SUR UN RÉSEAU DE TÉLÉPHONIE MOBILE, NOTAMMENT À LA NORME "GSM", ET SYSTÈME EMBARQUÉ À PUCE ÉLECTRONIQUE.			
LE(S) DEMANDEUR(S) :			
BULL CP8 BP 45 - 68, route de Versailles 78430 LOUVECIENNES - FRANCE			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		NACHEF	
Prénoms		Armand	
Adresse	Rue	21 boulevard Vauban	
	Code postal et ville	78180	Montigny le Bretonneux - FRANCE
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Louveciennes, le 20 juin 2000  CORLU Bernard (Mandataire)	

CET AVAILABLE CO

## DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
26 à 28	29		X	15/10/01	07 AVR. 2005 / TFA

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifiées).



L'invention concerne un procédé de traitement et de transmission de données numériques sur un réseau de téléphonie mobile.

Elle s'applique plus particulièrement à un réseau de téléphonie mobile conforme à la norme "GSM" (acronyme pour "Groupe spécial  
5 Systèmes Mobiles publics de radiocommunications fonctionnant dans la bande des 900 MHz).

L'invention concerne encore un système embarqué muni d'une puce électronique pour la mise en œuvre du procédé.

Dans le cadre de l'invention, le terme "réseau" doit être compris  
10 dans son sens le plus général. Il inclut les composants de transmission proprement dits du réseau (sous-systèmes de radiotransmission, câbles de transmissions, faisceaux hertziens, sous-systèmes "filaires" terrestres, etc.), mais aussi tous les systèmes raccordés au réseau de téléphonie mobile (stations de base, contrôleurs de station, commutateurs, annuaires, etc., et,  
15 de façon plus générale, tous systèmes de traitement informatique de données et serveurs raccordés au réseau), y compris les postes, équipements ou stations mobiles détenus par les utilisateurs (abonnés) du réseau de téléphonie mobile.

Ces derniers dispositifs peuvent être des téléphones portatifs ou  
20 des terminaux plus complexes, par exemple un terminal cumulant les fonctionnalités de téléphone et d'organiseur. Pour simplifier, sans restreindre en quoi que ce soit la portée de l'invention, ces dispositifs seront appelés ci-après "téléphones mobiles". Les téléphones mobiles sont munis, notamment, d'un système embarqué muni de moyens de traitement de  
25 l'information et de mémorisation, incluant un module fonctionnel connu sous l'abréviation "SIM" (pour "Subscriber Identity Module" ou "Module d'identification d'abonné"). Egalement pour simplifier, on supposera ci-après que le module "SIM" est porté par une carte à puce. Un logiciel d'exploitation de la carte à puce est également prévu (dit "OS", pour "Operating System").

30 Dans l'état actuel des techniques, les téléphones mobiles des réseaux "GSM" ne sont plus seulement utilisés pour téléphoner. On peut les utiliser aussi pour traiter et envoyer des données numériques, notamment

sous la forme de courts messages (service dit "GSM-Data"). Ces messages ont typiquement une longueur de 160 septets ou de 140 octets, selon les applications.

5 Récemment, on a assisté à l'apparition d'une technologie normalisée dite "Sim Toolkit". Cette technologie fait d'ores et déjà partie des services complémentaires offerts par certains opérateurs de téléphonie mobile des réseaux "GSM". De façon pratique, une pièce de logiciel spécifique est implémentée dans la carte à puce "SIM" du téléphone.

10 Cette norme permet aux applications, qui tournent sur la carte à puce ("SIM") des téléphones mobiles, d'envoyer des commandes à l'équipement mobile associé de type :

- . afficher un texte sur l'écran du téléphone mobile ;
- . demander à l'utilisateur de taper du texte comme entrée de l'application
- 15 . demander l'appel téléphonique d'un numéro ;
- . demander l'envoi d'un message court qui contient du texte ou des données, à un serveur ou à un autre téléphone ;
- . demander l'exécution d'une commande sur une carte à puces auxiliaire dans l'équipement mobile ;
- 20 . etc.

Ces commandes sont appelées commandes "pro-actives".

La norme "Sim Toolkit" permet aussi aux applications de la carte à puce "SIM" de réagir suite à la réception d'un certain nombre d'événements provenant de l'équipement mobile. Ces événements sont de type :

- 25 . sélection de l'application à partir d'une commande dite de "MENU" qui se trouve sur un clavier dont sont munis les équipements mobiles ;
- . réception d'un message court à destination d'une application ou du système d'exploitation de la carte à puce "SIM" ;
- . expiration du temps programmé dans une minuterie de l'équipement mobile ;
- 30 . demande d'appel d'un numéro téléphonique ;
- . etc.

Les fonctionnalités apportées par cette norme permettent de développer un très grand nombre d'applications distinctes sur la carte à puce, ce dans le but de fournir aux utilisateurs des services dits "à valeur ajoutée".

5 Pour une description plus détaillée de la technologie "Sim Toolkit", on se reportera avec profit à la norme "GSM 11.14".

En résumé, dans l'état de la technique actuelle, le standard "Sim Toolkit" consiste à développer des applications sur la carte à puce qui sont capables, à la fois, de commander l'équipement mobile supportant la carte à puce et aussi de réagir à des événements provenant de cet équipement. Ce  
10 standard est aujourd'hui adopté par la majorité des constructeurs d'équipements mobiles et de cartes à puces. C'est un standard qui permet d'écrire des applications à la fois puissantes et sécurisées.

Une application "Sim Toolkit" communique en général avec une ou  
15 plusieurs applications installées sur des serveurs, via le canal des messages courts. Ce canal est indépendant de celui de la voix et est standardisé par la norme "GSM". Les applications, qu'elles soient installées sur la carte "SIM" ou sur le serveur, peuvent à la fois envoyer et recevoir des messages courts qui contiennent du texte ou des données en format binaire.  
20 (Pour plus d'information sur les messages court en mode point à point, voir la norme "GSM 03.40")

Cependant, et bien que le nombre et la nature des services "GSM" à valeur ajoutée précités s'avèrent *a priori* sans limitation, les opérateurs téléphoniques et les développeurs d'applications logicielles sont  
25 constamment freinés par la limitation des ressources disponibles sur la carte à puce.

En effet, les deux inconvénients principaux présentés par la technologie "Sim Toolkit" sont :

1) la mémoire insuffisante des cartes à puce pour héberger des  
30 applications "Sim Toolkit", car celles-ci ne comportent que quelques dizaines de kilo-octets en mémoire : malgré toutes les optimisations effectuées par des développeurs d'applications logicielles très expérimentés,

les opérateurs de services de téléphonie buttent sur ce manque de mémoire pour charger et/ou exécuter des applications "Sim Toolkit" en grand nombre ; et

5                   2) le temps de réponse très élevé des cartes à puces : en effet, c'est à la carte à puce, qui est dotée d'une puissance de calcul moindre comparée aux processeurs des équipements mobiles et surtout des serveurs, que cette technologie impose d'effectuer les calculs les plus compliqués, lors de l'exécution des applications précitées.

10                   Or, il est clair que les besoins qui se font sentir vont dans une direction opposée. Tout d'abord, les opérateurs de téléphonie souhaitent mettre à la disposition de leurs abonnés le plus grand nombre possible de services annexes supplémentaires. En outre, les opérations effectuées par la carte à puce doivent l'être dans un temps minimum. La multiplication des applications disponibles, dans la mesure d'ailleurs où cette multiplication est  
15 possible, risque d'ailleurs de dégrader les performances en rendant le temps de traitement encore plus long, du fait de mutuelles interactions.

                  Malgré des progrès importants de la technologie des cartes à puce, déjà constatés dans une période récente, et prévisibles dans un avenir proche, les facteurs de limitation précités restent et resteront un frein  
20 important.

                  Une deuxième technologie standardisée, appelée "WAP" (pour "Wireless Application Protocol"), a été proposée récemment. Ce standard a pour but de permettre aux utilisateurs des téléphones mobiles d'accéder au réseau Internet à partir de leurs téléphones mobiles, via une liaison sans fil.

25                   Cette technologie n'est pas sans inconvénients.

                  Tout d'abord, il est nécessaire d'installer un navigateur "WAP", de type spécifique, car il présente des caractéristiques différentes des navigateurs de type "WEB" classiques. Ce navigateur est installé sur l'équipement mobile qui, certes possède plus de mémoire que la carte à  
30 puce, mais généralement beaucoup moins qu'un micro-ordinateur et naturellement qu'un serveur. En outre, bien que cette technologie présente l'avantage de permettre l'accès au réseau Internet, elle ne couvre pas toutes

les fonctionnalités des applications "Sim Toolkit". A titre d'exemple non limitatif, une application "WAP" ne peut pas, comme dans le cas des applications "Sim Toolkit", commander les appels téléphoniques. De plus, une application "WAP" ne peut pas garantir le même degré de sécurité que celui offert par les applications "Sim Toolkit". En effet, celles-ci utilisent des clés secrètes enregistrées dans les cartes à puce "SIM". Par exemple, une application "WAP" ne peut pas demander l'authentification d'une application sur un serveur quelconque. Ce n'est d'ailleurs pas la seule fonction de sécurité dévolue à la carte à puce "SIM". Elle assure également la sécurité et la confidentialité des informations transmises.

Pour assurer toutes ces fonctions, la carte à puce stocke un certain nombre de données dites "sensibles", des algorithmes de chiffrement et des clés associées, notamment :

- le numéro international d'abonné ou "IMSI" (pour "International Mobile Subscriber Identity") ;
- l'identité temporaire attribuée à une station mobile lors de son déplacement ou "TMSI" (pour "Temporary Mobile Subscriber Identity") ;
- une clé d'authentification individuelle, une clé de chiffrement utilisée pour chiffrer et déchiffrer des données dites de signalisations et de trafic sur la voie radio et trois algorithmes distincts de chiffrement et déchiffrement ou de génération de clés ; et
- un nombre de séquences de clés de chiffrement ou "CKSN" (pour "Ciphering Key Sequential Number"), indiquant la valeur de chiffrement ci-dessus valable pour éviter l'utilisation de clés différentes par la station mobile et le réseau.

Le fait que ces informations ou données sensibles soient stockées dans la carte à puce et que les traitements correspondants soient effectués dans celle-ci permettent d'obtenir un haut degré de sécurité et de confidentialité.

Enfin, dans l'état actuel des techniques, le coût des équipements mobiles qui supportent la technologie "WAP" reste élevé, si on le compare au coût de ceux qui supportent la technologie "Sim Toolkit".

5 L'invention vise à pallier les inconvénients des dispositifs et systèmes de l'art connu, et dont certains viennent d'être rappelés, tout en satisfaisant aux besoins qui se font sentir.

10 L'invention se fixe pour but un procédé de traitement et de transmission de données numériques sur un réseau de téléphonie mobile, notamment à la norme "GSM" permettant d'apporter aux utilisateurs des téléphones mobiles sur ce réseau, tous les services qu'on peut offrir avec les applications conforme à la technologie "Sim Toolkit", mais en s'affranchissant des limitations de mémoires et de performances rencontrées lors du développement des applications sur les cartes à puces, pour le moins en grande partie.

15 Pour ce faire, l'invention tire avantageusement parti du fait que les applications conformes à la technologie "Sim Toolkit" peuvent notamment envoyer des messages courts et aussi entreprendre l'exécution d'instructions, suite à la réception d'autres messages courts qui leur sont destinées.

20 L'architecture de réseau de téléphonie mobile selon l'invention est une architecture dans laquelle des applications "Sim Toolkit" :

1) informent des applications installées sur au moins un serveur éloigné, raccordé au dit réseau de téléphonie, de l'arrivée d'événements provenant d'un équipement mobile : ces applications seront appelées ci-  
25 après "applications Sim Toolkit rapporteuses" ; et

2) exécutent des commandes et des instructions suite à la demande d'applications implémentées sur lesdits serveurs : ces dernières applications seront appelées ci-après "applications Sim Toolkit esclaves".

De cette manière, on peut déléguer l'exécution de traitements  
30 lourds, grands consommateurs de ressources informatiques, qui s'effectuent, dans l'art connu, sur la carte à puce "SIM", à des applications implémentées sur ces serveurs.

Les serveurs précités ne présentent pas *a priori* de limitations intrinsèques, comme dans le cas des cartes à puce "SIM", ni en ce qui concerne la quantité de mémoire disponible, ni en ce qui concerne la puissance de calcul. Le nombre d'applications "Sim Toolkit" disponibles via une carte à puce "SIM" (et donc le nombre de services offerts) peut alors être fortement augmenté, tout en permettant une grande vitesse de traitement.

Par ailleurs, les fonctionnalités liées à la sécurité et la confidentialité restant confinées dans la carte à puce "SIM", comme dans l'art connu, un haut niveau de qualité de service continue d'être garanti.

L'invention a donc pour objet principal un procédé de transmission et de traitement de données numériques sur un réseau de téléphonie mobile, ledit réseau comprenant au moins un équipement mobile et un serveur éloigné comprenant des moyens de traitement d'information et de stockage de données, communiquant entre eux via ledit réseau de téléphonie mobile, ledit équipement mobile coopérant avec un système embarqué à puce électronique comprenant des moyens de traitement d'information et de stockage de données destinés à mémoriser au moins des pièces de logiciel d'un type capable, tout à la fois, de commander ledit équipement mobile par l'émission de commandes déterminées et de réagir à des événements provenant de cet équipement par exécution d'instructions associées à ces dits événements, en vue de réaliser des fonctionnalités associées à au moins une application prédéterminée, caractérisé en ce qu'il comprend l'implémentation d'au moins une première pièce de logiciel particulière, d'un type dit rapporteur, stockée dans lesdits moyens de stockage de données dudit système embarqué à puce électronique, et l'implémentation d'au moins une pièce de logiciel associée stockée dans lesdits moyens de stockage de données de l'un desdits serveurs éloignés, en ce que ladite pièce de logiciel de type rapporteur retransmet à ladite pièce de logiciel associée des données caractéristiques desdits événements reçus dudit équipement mobile et en ce que cette pièce de logiciel associée exécute, par l'intermédiaire desdits moyens de traitement d'information dudit

serveur éloigné, sur réception desdites données caractéristiques, tout ou partie desdites instructions associées à l'une desdites applications prédéterminées et retransmet des résultats de ladite exécution au dit équipement mobile et/ou au dit système embarqué à puce électronique.

5 L'invention a encore pour objet un système embarqué muni d'une puce électronique coopérant avec un équipement mobile connecté au dit réseau de téléphonie mobile.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

10 - la figure 1 est un diagramme illustrant schématiquement les principales étapes de l'activation d'une application "Sim Toolkit" située sur un serveur éloigné par une application, selon un aspect de l'invention d'un premier type dit "rapporteur", située sur une carte à puce "SIM" ;

15 - La figure 2 est un diagramme illustrant schématiquement l'interrelation selon l'invention, entre une application située sur un serveur éloigné, d'un type dit "maître", et une application "Sim Toolkit" située sur une carte à puce "SIM", d'un deuxième type dit "esclave", selon un autre aspect de l'invention ;

20 - la figure 3 est un diagramme illustrant les principales étapes du procédé selon l'invention d'envoi d'une commande "pro-active" conforme à la norme "GSM 11.14" ;

25 - la figure 4 est un diagramme explicitant, pour un exemple particulier, les principales étapes d'échanges de données et de commandes entre une application "Sim Toolkit" située sur une carte à puce "SIM" et une application située sur un serveur éloigné, selon l'art connu ; et

30 - la figure 5 est un diagramme explicitant, pour cet exemple particulier, les principales étapes d'échanges de données et de commandes entre une application "Sim Toolkit" située sur une carte à puce "SIM" et une application située sur un serveur éloigné, selon le procédé de l'invention.



On va maintenant décrire de façon plus détaillée un exemple de réalisation préférée d'architecture de réseau de téléphonie mobile selon l'invention.

5 Comme il a été indiqué, selon l'une des caractéristiques de l'invention, on délègue l'exécution de traitements lourds, qui s'effectuent dans l'art connu sur la carte "SIM", à des applications implémentées sur un ou plusieurs serveurs éloignés connectés au réseau.

10 Selon une autre caractéristique de l'invention, on prévoit deux catégories principales d'applications "Sim Toolkit" que l'on a appelé "Applications Sim Toolkit rapporteuses" et "Applications Sim Toolkit esclaves", respectivement, toutes deux implémentées sur les cartes à puce "SIM".

On va maintenant décrire de façon plus détaillée les deux types d'application.

15 Application "Sim Toolkit" rapporteuse

Une application "Sim Toolkit" réagit en premier lieu aux événements provenant du téléphone mobile, ou de façon plus générale de l'équipement mobile de l'abonné. Ces événements arrivent à la carte à puce "SIM" dans une commande connue sous la dénomination anglo-saxonne "Envelope". La commande "Envelope" peut contenir, par exemple, l'événement "Menu Selection", avec comme indice de sélection celui de cette application "Sim Toolkit". Cet événement permet donc de choisir une application dans un menu qui s'affiche sur des moyens de visualisation dont est pourvu le téléphone mobile. Une description plus détaillée de cette commande peut être trouvée dans la norme "GSM 11.14".

20

25

L'équipement mobile n'a aucune connaissance des applications qui se trouvent sur les serveurs. Pour faire réagir une application sur un serveur aux événements définis dans la norme "Sim Toolkit", il est nécessaire de la coupler avec une application "Sim Toolkit" installée sur la carte "SIM", que l'on appellera ci-après "application Sim Toolkit rapporteuse". L'équipement mobile voit l'application rapporteuse comme si elle était une application "Sim Toolkit" classique. Il n'a aucune connaissance de l'application

30

correspondante située sur un serveur. De ce point de vue, il y a transparence totale.

5 L'application rapporteuse s'inscrit dans la carte "SIM" pour se mettre à l'écoute des événements auxquels son application correspondante implémentée sur un serveur doit réagir. Dès que l'application rapporteuse reçoit un événement provenant de l'équipement mobile, elle prépare un message court à destination de son application correspondante. Ce message court contient toutes les données caractérisant l'événement reçu. Son envoi est réalisé de façon pratique par une commande du type  
10 "commande pro-active" précité.

L'application correspondante du serveur reçoit le message court. Ce message l'informe de l'arrivée d'un événement venant de l'équipement mobile. Elle entreprend alors le traitement relatif à la réception de cet événement. Ce traitement peut consister, par exemple, à se connecter à un  
15 site "WEB". Elle peut aussi devenir une application dite maître d'une autre application dite esclave implémentée sur la carte à puce "SIM". Elle peut par conséquent commander l'application esclave, pour qu'elle envoie des commandes "pro-actives" à l'équipement mobile et aussi pour qu'elle invoque des méthodes stockées dans bibliothèques installées sur la carte à  
20 puce "SIM".

La figure 1 est un diagramme illustrant schématiquement les principales étapes de l'activation d'une application "Sim Toolkit" 30M située sur un serveur éloigné 3 par une application de type "Sim Toolkit rapporteuse" 21 située sur une carte à puce "SIM" 2 d'un équipement mobile  
25 1. Le serveur éloigné 3 et l'équipement mobile 1 de l'abonné Ab sont tous deux connectés à un réseau de téléphonie mobile RT (non explicitement représenté). Ce réseau, bien connu de l'Homme de Métier, et classique en soi, ne nécessite aucune modification qui serait due au procédé de l'invention. Il s'ensuit que, *a priori*, tous les réseaux conformes à l'art connu  
30 conviennent, ce qui représente d'ailleurs un avantage supplémentaire de l'invention. Il n'est donc pas nécessaire de décrire plus avant un tel réseau et ses différents composants. On pourra se référer avec profit, à titre

d'exemple non limitatif, à l'article de Jean CELLMER, intitulé "Réseaux cellulaires, Système GSM", paru dans les "Techniques de l'Ingénieur", Volume TE 7364, novembre 1999, pages 1 à 23.

L'équipement mobile 1, par exemple un poste téléphonique portable, comprend des circuits électroniques classiques (mémoires, processeur, etc.) 10. Ces derniers peuvent être couplés à une carte à puce "SIM" 2 à l'aide d'un lecteur (non représenté). La carte à puce "SIM" 2 comprend également des circuits électroniques 20, notamment un processeur et des moyens de mémoires dans lesquels peuvent être enregistrées des applications "Sim Toolkit" que l'on appellera classiques (non représentées), car communes en soi à l'art connu, ainsi qu'une ou plusieurs applications "Sim Toolkit" rapporteuses 21 conformes à l'une des caractéristiques de l'invention. Sur la figure 1, pour illustrer le processus simplement, une seule application a été représentée, à l'extérieure des circuits 20 de la carte à puce "SIM" 2. Dans la réalité, cette application 21 est stockée, comme les applications de type classique, dans les moyens de mémoire de la carte à puce 2.

Les étapes précitées sont les suivantes (symbolisées par des flèches en trait plein sur la figure 1) :

- F1) les circuits 10 de l'équipement mobile 1 envoient une commande de type "Enveloppe" aux circuits 20 de la carte à puce "SIM" 2 : cette commande "Enveloppe" contient un des événements prévus par la norme GSM 11.14 précitée ;
- F2) les circuits 20 de la carte "SIM" 2 envoient cet événement à une application "Sim Toolkit" rapporteuse 21 apte à y répondre ; et
- F3) l'application "Sim Toolkit" rapporteuse 21 envoie ce même événement, dans un message court, à une application correspondante 30M située dans le serveur 3 qui va la traiter, via le réseau RT.

Pour des raisons qui seront explicitées ci-après, l'application 30M sera appelée "application maître".

### Application "Sim Toolkit" esclave

De façon connue en soi, une application "Sim Toolkit" de l'art connu peut notamment :

- 5           a) envoyer des commandes "pro-actives" conformes à la norme "GSM 11.14" à l'équipement mobile : elle peut, par exemple, demander à l'équipement mobile d'afficher du texte ;
- b) envoyer des commandes conformes à la norme "GSM 11.11" précitée au système d'exploitation de la carte à puce "SIM", sans passer par l'équipement mobile ; et
- 10          c) demander l'exécution de méthodes stockées dans des bibliothèques implémentées sur la carte à puce "SIM" : elle peut par exemple appeler une méthode de la carte à puce "SIM" pour demander le chiffrement d'un message à l'aide d'une clé secrète stockée sur cette carte.

15           Selon un aspect supplémentaire de l'invention, les applications implémentées sur les serveurs éloignés sont dotées de ces fonctionnalités. Il est ainsi possible de leur déléguer le traitement qui s'effectue, dans l'art connu, en ayant recours à une application "Sim Toolkit" classique implémentée sur la carte à puce.

20           Pour qu'une application implémentée sur le serveur éloigné 3 puisse effectuer ces opérations, il est nécessaire qu'elle puisse communiquer avec une application "Sim Toolkit" implémentée sur la carte à puce "SIM" 2. Elle envoie alors des commandes à cette dernière application qui les exécute. On appellera ci-après les applications implémentées sur les serveurs éloignés "Applications maîtres» et les applications "Sim Toolkit" installées sur la carte à puce "SIM" "Application Sim Toolkit esclaves".

25           La figure 2 est un diagramme illustrant schématiquement l'interrelation entre ces deux types d'applications.

          Une application "Maître" 30M envoie une commande (trait plein sur la figure 2) à une application "Sim Toolkit esclave" 22. Cette dernière application exécute la commande, puis répond à l'application "Maître" 30M,

en lui retournant le résultat de la commande (trait discontinu) après traitement.

On va maintenant décrire de façon détaillée comment une application "Maître" 30M peut envoyer des commandes des types a) à c) précitées.

Envoi d'une commande "pro-active" conforme à la norme "GSM 11.14"

Les principales étapes du procédé selon l'invention sont explicitées ci-dessous, par référence au diagramme de la figure 3 :

- 10 a) une application maître 30M prépare une commande "pro-active" afin qu'elle soit exécutée par les circuits 10 d'un équipement mobile 1 : elle l'inclut dans des données d'un message court à destination d'une application "Sim Toolkit" esclave 22 (via les circuits 10 d'un équipement mobile 1, sur lequel la commande "pro-active" est
- 15 exécutée) - flèches F'1 et F'2 sur la figure 3 - ;
- b) l'application "Sim Toolkit" esclave 22 analyse les données du message court reçu : elle comprend que l'application maître 30M lui demande d'envoyer la commande "pro-active" aux circuits 10 de son équipement mobile 1, elle transfère alors cette commande à
- 20 l'équipement mobile 1 et se bloque en attente d'une réponse en retour - flèche F'3 - ;
- c) les circuits 10 de l'équipement mobile 1 reçoivent la commande "pro-active" : ils l'exécutent et envoient une réponse à la carte "SIM" 2, sous forme d'une commande communément appelée "Terminal
- 25 Response" – flèche F'4 - , cette commande contenant le résultat de l'exécution de la commande "pro-active" par les circuits 10 de l'équipement mobile 1 (par exemple, si la commande "pro-active" consiste à demander de mettre sous-tension une carte à puce auxiliaire, non représentée, sur l'équipement mobile 1, le résultat
- 30 envoyé dans la commande "Terminal Response" contient une suite d'octets qui est la réponse d'une mise à zéro de la carte auxiliaire) ;

- d) l'application "Sim Toolkit" esclave 22 qui est restée bloquée après l'envoi de la commande "pro-active", se débloque suite à la réception de la commande "Terminal Response" précitée ;
- e) l'application "Sim Toolkit" esclave 22 prépare un message court contenant le résultat de la commande "pro-active" qu'elle trouve dans la commande "Terminal Response" provenant des circuits 10 de l'équipement mobile 1 ;
- f) l'application "Sim Toolkit" esclave 22 envoie ce message court, dans une commande "pro-active", à destination de l'application maître 30M, via les circuits 10 de l'équipement mobile 1 - flèche F'5 - ;
- g) les circuits 10 de l'équipement mobile 1 transfèrent le message court vers l'application maître 30M - flèche F'6 ; et
- h) l'application maître 30M le reçoit et traite la réponse de la commande "pro-active" qu'elle a précédemment envoyée.

**15**            Envoi d'une commande non "pro-active", c'est-à-dire conforme à la norme "GSM 11.11"

L'application maître 30M (figure 3) peut envoyer des commandes "GSM 11.11" à la carte à puce "SIM" 2 suivant deux méthodes différentes, ces deux méthodes pouvant être utilisées indifféremment.

**20**            Méthode 1

- a) une application maître 30M prépare une commande, selon la norme "GSM 11.11", à destination d'une application "Sim Toolkit" esclave 22 implémentée sur la carte à puce "SIM" 2 : elle l'envoie dans un message court, via les circuits 10 de l'équipement mobile 1 ;
- b) l'application "Sim Toolkit" esclave 22 analyse les données du message court reçu : elle transmet la commande trouvée dans ce message au système d'exploitation 23 de la carte à puce "SIM" 2 ;
- c) le système d'exploitation 23 de la carte à puce "SIM" 2 exécute la commande qui vient de l'application "Sim Toolkit" esclave 22 et retourne une réponse à cette commande à cette application 22 ;
- d) l'application "Sim Toolkit" esclave 22 prépare un message court ayant comme destination une application maître correspondante 30M,

implémentée sur le serveur éloigné 3 : ce message contient le résultat de la commande "GSM 11.11" et est envoyé par l'application esclave aux circuits 10 de l'équipement mobile 1, dans une commande "pro-active" ;

5 e) les circuits 10 de l'équipement mobile 1 transfèrent le message court à l'adresse du destinataire, indiquée dans le message lui-même, c'est-à-dire l'application maître 30M ; et

f) l'application maître 30M le reçoit et traite la réponse reçue.

### Méthode 2

10 L'application maître 30, implémentée sur le serveur éloigné 3, envoie directement une commande "GSM 11.11" dans un message court au système d'exploitation 23 de la carte à puce "SIM", selon les normes "GSM 03.40" et "GSM 03.48".

15 L'avantage de cette solution est sa simplicité car elle ne nécessite pas la présence d'une application "Sim Toolkit" esclave, comme dans le cas de la méthode 1.

Par contre, l'inconvénient de la méthode 2 est que très peu de systèmes d'exploitation de cartes à puce "SIM" implémentent pleinement cette fonctionnalité. En général, une application d'un serveur peut envoyer un scénario de commandes dans un message court pour être exécuté, mais 20 la carte à puce "SIM" ne retourne pas le résultat de la commande. Si, par exemple, l'application implémentée sur le serveur a besoin de connaître le contenu d'un fichier sur la carte à puce "SIM", elle ne le pourra pas, sur la majorité des cartes à puce "SIM".

### Appel d'une fonction d'une bibliothèque de la carte à puce "SIM"

25 Comme il a été indiqué, une application "Sim Toolkit" peut avoir besoin de demander l'exécution d'une fonction comprise dans une bibliothèque de la carte à puce "SIM" (opération c) précitée). Il existe deux catégories principales de fonctions dans une carte à puce "SIM" :

30 1) les fonctions qui font appel dans leurs paramètres à au moins une clé secrète stockée dans la carte à puces : ces fonctions sont utilisées pour chiffrer, déchiffrer, signer ou vérifier une signature ; et

2) les fonctions qui, au contraire, n'utilisent pas de clés secrètes.

Les fonctions de la première catégorie ne peuvent pas être déportées sur un serveur si on veut conserver un degré élevé de sécurité, comme il a été rappelé. Une application esclave 22 (figure 3) doit être capable de les appeler suite à une demande de l'application maître 30M.

5 Une convention doit exister entre l'application esclave 22 et l'application maître 30M pour permettre à cette dernière d'effectuer des opérations de chiffrement/déchiffrement et de signature avec des clés secrètes de la carte à puce "SIM" 2.

10 Par exemple, l'application maître 30M envoie un message à l'application esclave 22 dans lequel elle indique la nature de la fonction de cryptologie à effectuer (par exemple un chiffrement faisant appel à l'algorithme connu sous le sigle anglo-saxon "DES", pour "Data Encryption System"). Elle indique aussi les références de la clé à utiliser, stockée dans la carte à puce "SIM" 2 et le message à chiffrer. L'application esclave 22  
15 appelle la fonction de chiffrement appropriée et retourne le résultat à l'application maître 30M.

Pour la deuxième catégorie de fonctions, il est possible de faire appel à la même méthode que celle utilisée pour la première catégorie, mais, conformément à une caractéristique avantageuse de l'invention, ces  
20 fonctions sont implémentées directement sur un serveur éloigné 3. L'avantage de cette solution est que le traitement se fait sans aucun besoin de connexion, sur une machine *a priori* beaucoup plus puissante que la carte à puce "SIM" 2.

Conformément à l'une des caractéristiques de l'invention, une partie  
25 des applications "Sim Toolkit" est implémentée directement sur un ou plusieurs serveurs éloignés 3. Pour assurer une migration aisée de ces applications "Sim Toolkit" à partir des cartes à puces "SIM", il est également nécessaire d'implémenter toutes les fonctions associées qui se trouvent dans des bibliothèques de la carte à puce "SIM".

30 Pour fixer les idées, si on considère des cartes dites "Java" (marque déposée), ces fonctions sont constituées par des "APIs Javacard", des "APIs GSM 03.19", ainsi que des "APIs" dits "propriétaires", c'est-à-dire



spécifiques. "Java" est un langage de programmation orienté objet développé par la société "Sun Microsystems Inc." et les "APIs" sont des interfaces programmables avec les applications. Le langage "java" permet notamment de développer de courtes applications connues sous le sigle anglo-saxon "applet" ("appliquettes"). Les applications "Sim Toolkit" peuvent être réalisées à base "d'applets".

Par ces dispositions propres à l'invention, il est possible d'assurer qu'une application en technologie "Sim Toolkit" existante, qui s'exécute dans l'art connu sur une carte à puce "SIM", s'exécutera également sur un serveur éloigné, ce sans qu'il soit nécessaire de modifier une ligne de code, ce qui constitue un avantage supplémentaire de l'invention.

Il a été supposé jusqu'à ce point que la technologie dite des messages courts (c'est-à-dire conforme à la norme "GSM 03.40") était mise en œuvre comme technologie de transport. Le recours à cette technologie est avantageux car :

- 1) elle est très répandue aujourd'hui dans les réseaux "GSM" ; et
- 2) elle est disponible parmi les événements et les commandes "pro-actives" de la norme "Sim Toolkit" (c'est-à-dire conforme à la norme "GSM 11.14").

Cependant, il doit être clair qu'il est possible de mettre en œuvre bien d'autres technologies de transport sur des liaisons de transmission sans fil qui existent entre une carte à puce "SIM" et un serveur éloigné, technologies actuellement disponibles ou qui le seront dans le future

Les mécanismes des applications "Sim Toolkit" esclaves et rapporteuses définis ci-dessus ne nécessiteront pas de modifications, ce qui assure une grande pérennité au procédé selon l'invention.

Dans le mécanisme des applications "Sim Toolkit" esclave et maître, l'application "Sim Toolkit" esclave a été supposée complètement esclave. Il est possible d'envisager, tout en restant dans le cadre de l'invention, des applications "Sim Toolkit" esclaves possédant aussi une certaine "intelligence". Ce type d'application, que l'on pourra appeler "hybride" est alors capable, à la fois, d'obéir à une application maître et

d'effectuer des traitements locaux de façon autonome. En effet, une application "Sim Toolkit", fusse-t-elle de type esclave, continue de posséder les possibilités inhérentes aux applications "Sim Toolkit" classiques.

5 De même, il est possible d'adjoindre une fonctionnalité de type similaire, c'est-à-dire une certaine "intelligence", aux applications rapporteuses.

On est amené à constater que le fait de déporter des fonctionnalités applicatives d'une carte à puce "SIM" vers un serveur éloigné augmente le trafic sur le réseau et peut avoir, dans certaines conditions défavorables, des conséquences non négligeables sur les temps de réponse, car le débit  
10 du protocole des messages courts est faible.

Aussi, dans la pratique, on préfère le plus souvent des applications "Sim Toolkit" qui sont à la fois esclaves et autonomes, et/ou des applications "Sim Toolkit" qui sont à la fois rapporteuses et autonomes, ce qui permet de  
15 minimiser l'impact négatif de l'augmentation de trafic précité.

De façon pratique également, on cherche à trouver un compromis entre l'utilisation des ressources de la carte à puce "SIM" et l'envoi des messages courts qui peut s'avérer pénalisant en terme de performance.

On doit également noter que des authentifications entre les applications "Sim Toolkit" implémentées sur la carte à puce "SIM", qu'elles  
20 soient esclaves ou rapporteuses, et des applications implémentées directement sur un serveur doivent avoir lieu. Elles peuvent être réalisées en respectant la norme "GSM 03.48".

Cette norme prévoit aussi le chiffrement de certaines informations qui sont transportées lors des échanges entre une carte à puce "SIM" et un  
25 serveur éloigné.

En général, une application maître doit communiquer avec plusieurs applications esclaves. Pour ce faire, il est avantageux d'avoir recours à la technique dite de «Threads» lors de l'implémentation des "APIs" sur les  
30 serveurs.

Dans l'état actuel des techniques, les cartes à puce "SIM", de type "Java" précité, qui implémentent la norme "GSM 03.19", ne savent pas

envoyer une commande aux équipements mobiles sans passer par une classe d'objet connue sous la dénomination "sim.toolkit.ProactiveHandler". Lorsqu'une application "Sim Toolkit" esclave reçoit une commande "pro-active" envoyée par une application maître, elle doit la reconstruire en utilisant des méthodes d'une classe objet connue sous la dénomination "ProactiveHandler". On constate qu'il est donc nécessaire de ré-effectuer tout le travail préparé par le serveur qui a envoyé la commande, ce avant d'envoyer une commande "pro-active" à l'équipement mobile.

Pour que le mécanisme des applications esclaves et maîtres, selon une des caractéristiques de l'invention, conserve tous ses avantages, on implémente avantageusement sur la carte à puce "SIM", une fonction qui ne fait qu'envoyer à l'équipement mobile une commande "pro-active" à partir d'un tableau d'octets quelconque. L'application "Sim Toolkit" esclave peut alors accepter la commande "pro-active" reçue, commande qui était préparée et envoyée par l'application maître. Elle l'envoie ensuite à l'équipement mobile sans devoir effectuer aucun traitement supplémentaire.

#### Exemple de réalisation pratique

On va maintenant décrire de façon plus détaillée un exemple de réalisation pratique par référence aux figures 4 et 5.

On suppose que l'on désire accéder à  $n$  services implémentés sur un serveur de messages courts. Ces services seront appelés ci-après, de façon arbitraire, *Service 1*, *Service 2*, ..., *Service n*. On suppose que les applications "Sim Toolkit" sont réalisées à base d'applets "Java".

Le développement d'une telle application avec la technologie "Sim Toolkit" classique, c'est-à-dire conforme à l'art connu, nécessite le développement :

- 1) d'une application "Sim Toolkit", que l'on peut appeler "AppST", implémentée sur une carte à puce "SIM" ; et
- 2) d'une autre application, que l'on peut appeler "AppOTA", implémentée sur un serveur éloigné, que l'on appellera "OTA" (pour "Over The Air").

L'application "AppST" répond à deux événements qui sont : "*Menu Selection*" (sélection de menu) et "*SMS PP Download*" (téléchargement de messages courts).

5        Quand l'application "AppST", reçoit l'événement "*Menu Selection*", elle envoie à l'équipement mobile une commande "pro-active" dénommée "*Select Item*", c'est-à-dire la sélection d'un item du menu (un service) parmi les  $n$  services proposés.

10       L'utilisateur choisit par exemple le service de rang ou indice arbitraire  $i$ , ou *Service i*. Une applet de l'application "AppST" envoie, dans une commande "pro-active", un message court à l'application "AppOTA" lui indiquant que l'utilisateur demande le service *Service i*.

L'application "AppOTA" reçoit le message court venant de l'application "AppST" et lui répond en lui retournant le contenu de *Service i* dans un autre message court.

15       Quand l'application "AppST" reçoit le message court venant de l'application "AppOTA", elle envoie une commande "pro-active" de type dit "*Display Text*" (affichage de texte) pour afficher son contenu sur l'écran du mobile.

20       La figure 4 est un diagramme illustrant schématiquement les huit étapes précédentes, conformes à l'art connu :

Etape 1 : envoi par les circuits 10 de l'équipement mobile 1 de "*Menu Selection Event*" à l'application "AppST" 30' ;

Etape 2 : envoi par l'application "AppST" 30' de "*Select Item*" aux circuits 10 de l'équipement mobile 1 ;

25       Etape 3 : réponse de ces circuits par l'envoi de "*Terminal response*" à l'application "AppST" 30' ;

Etape 4 : envoi par celle-ci de "*Send SM (indice i)*" (envoyer message court d'indice  $i$ ) à l'application "AppST" 30' ;

30       Etape 5 : envoi par ces derniers de "*Short Msg (indice i)*" (envoi du message court d'indice  $i$ ) à l'application "AppOTA" 21' ;

Etape 6 : réponse de celle-ci et envoi de "*Short Msg (Service 'i')*" (message court pour le service d'indice " $i$ ") ;

Etape 7 : envoi par les circuits 10 de l'équipement mobile 1 de "SMS PP Download Event" à l'application "AppST" 30' ; et

5      Etape 8 : envoi par l'application de "AppST" 30' de "Display Text (Service "i")" aux circuits 10 de l'équipement mobile 1 pour affichage du contenu du message court associé au service d'indice "i" pour l'affichage du contenu sur un écran 11 de l'équipement mobile 1.

10      Le développement de cette même application, selon le procédé de l'invention, s'effectue de la façon décrite ci-dessous, en regard de la figure 5.

On installe sur la carte à puce 2 deux applications "Sim Toolkit" constituées par des applets "Java" : la première est l'application rapporteuse 21 qui transmet les événements reçus dans des messages courts à une application correspondante, ou application maître 30M du serveur 3.

15      La deuxième est l'application esclave 22 qui exécute les ordres de l'application maître 30M du serveur 3.

Il est à remarquer que l'application maître 30M du serveur 3 joue le rôle des deux applications "AppST" et "AppOTA" de l'art connu décrit en regard de la figure 4.

20      Une fois que cette application 30M reçoit l'événement "Menu Selection", elle devient le maître de l'application "Sim Toolkit" esclave 22.

Elle lui demande d'abord de transmettre aux circuits 10 de l'équipement mobile 1 la commande "pro-active" "Select Item" précitée. Quand elle reçoit la réponse de cette commande, elle lui demande de  
25      nouveau d'exécuter la commande "pro-active" "Display Text" pour afficher le service sélectionné.

Le procédé selon l'invention, pour l'application décrite, comprend désormais douze étapes détaillées ci-après :

30      Etape 1 : envoi par les circuits 10 du mobile 1 de "Menu Selection Event" à l'application rapporteuse (cette étape est initiée par l'utilisateur de l'équipement mobile 1) ;

- Etape 2 : réponse et envoi par l'application rapporteuse 21 de "*Send SM (Menu Selection)*" (envoyer un message court de sélection de menu) aux circuits 10 du mobile 1 ;
- 5 Etape 3 : envoi par les circuits 10 du mobile 1 de "*SM (Menu Selection)*" à l'application 30M (partie "*AppST*" de cette application) ;
- Etape 4 : traitement et envoi par l'application 30M de "*SM(Select Item)*" aux circuits 10 du mobile 1 ;
- Etape 5 : envoi par ces derniers de "*SMS PP Download Event*" à l'application esclave 22 ;
- 10 Etape 6 : traitement par l'application esclave 22 et envoi de "*Select Item*" aux circuits 10 du mobile 1 ;
- Etape 7 : envoi par les circuits 10 du mobile 1 de "*Terminal Response (indice i)*" à l'application esclave 22 ;
- Etape 8 : envoi par cette dernière de "*Send SM (Indice 'i')*" aux circuits
- 15 10 du mobile 1 ;
- Etape 9 : envoi par les circuits 10 du mobile 1 de "*SM (selected indice 'i')*" (message court pour traitement à l'indice sélectionné "*i*") à l'application 30M (partie "*AppOTA*") ;
- Etape 10 : traitement et envoi par l'application 30M de "*SM(Display Text*
- 20 *Service 'i')*" aux circuits 10 du mobile 1 ;
- Etape 11 : envoi par ces derniers de "*SMS PP Download Event*" à l'application esclave 22 ; et
- Etape 12 : traitement et envoi de "*Display text (Service 'i')*" aux circuits 10 du mobile 1, pour affichage du contenu du message court.
- 25 La mise en œuvre du procédé selon l'invention induit une légère augmentation du trafic sur le réseau, puisque le nombre d'étapes est supérieur pour une même application. Cependant, l'application principale associée à un service déterminé a été déportée de la carte à puce "SIM" 2 vers le serveur 3. Il s'ensuit que le nombre de services n'est potentiellement
- 30 plus limité, puisqu'il n'est plus nécessaire de charger autant d'applets sur la carte à puce "SIM" 2. Les ressources en mémoire du serveur 3 sont en effet incomparablement supérieures à celles présentes dans la carte à puce

"SIM" 2. De même la vitesse de traitement est très grande, car le ou les processeurs présents sur le serveur 3 sont également beaucoup plus puissant que ceux que l'on peut implanter dans la carte à puce "SIM" 2.

5 En outre, suivant le contexte précis dans lequel il se trouve, un développeur d'applications logicielles conserve la possibilité de répartir de façon optimisée les traitements à réaliser entre la carte à puce "SIM" 2 et le serveur 3, selon un aspect supplémentaire avantageux de l'invention qui a été explicité.

10 Pour ce faire, certaines applications "Sim Toolkit" peuvent être laissées sur la carte à puce "SIM" 2. Ces d'applications fonctionnent de façon identique, ou pour le moins très similaire, aux applications de l'art connu.

15 Selon une autre variante de réalisation, permise par le procédé de l'invention, tout ou partie des applications esclaves 22 et/ou rapporteuses 21 peuvent être du type hybride précité, c'est-à-dire conserver une certaine autonomie. Il s'ensuit que, dans ce cas, une partie des traitements continue d'être réalisée en local, ce qui diminue en proportion le trafic entre la carte à puce "SIM" 2 et le ou les serveur(s) éloigné(s) 3.

20 A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

25 Elle permet notamment de déporter les traitements "lourds", grands consommateurs de ressources informatiques, sur des systèmes de traitements de données (serveurs éloignés) ne présentant pas de limitations, du moins de limitations importantes, notamment en moyens de stockage de données. En outre les traitements peuvent être effectués à grande vitesse, car les moyens de calculs présents sur ces systèmes sont également très rapides et puissants.

30 Selon un autre aspect de l'invention, bien que le procédé selon l'invention puisse impliquer un surplus de trafic, dans certaines conditions, cet inconvénient peut toutefois être fortement minimisé en optimisant la part des traitements déportés et la part des traitements restant effectués en local, c'est-à-dire sur la carte à puce "SIM" ou tout module en faisant fonction.

De ce fait, l'invention permet d'offrir un nombre virtuellement illimité de services sans devoir augmenter pour autant la quantité de données à stocker sur la carte à puce "SIM", ou pour le moins de façon marginale.

5 On doit aussi bien comprendre que les applications déportées précitées englobent des applications "Sim Toolkit" proprement dites, mais aussi des fichiers de données associés. A titre d'exemple, il peut être avantageux de déporter les données personnelles d'un utilisateur, ce que l'on nomme habituellement son "environnement", sur un serveur éloigné : carnet d'adresses, liste de numéros de téléphone, etc. Là encore, la taille de  
10 ces fichiers devient virtuellement illimitée.

On peut enfin remarquer, que l'invention présente l'avantage, lorsqu'une mise à jour d'une ou plusieurs application(s) doi(ven)t être effectuée(s), si celle(s)-ci est(sont) implantée(s) sur un serveur éloigné, cette mise à jour peut être réalisée par l'opérateur de façon très simple et  
15 rapide, car centralisée. Dans le cas d'applications "Sim Toolkit" standards, c'est-à-dire conformes à l'art connu, implantées sur les cartes à puce, la même opération nécessiteraient la modification de toutes les cartes à puce stockant les applications à mettre à jour, c'est-à-dire le plus souvent leur remplacement.

20 Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 1 à 3 et 5.

Elle n'est pas non plus limitée, comme il a été indiqué, seulement à des protocoles de transmission utilisant des messages courts.

25 Enfin, si elle s'applique avantageusement à des réseaux de téléphonie au standard "GSM", d'autres standards peuvent convenir, et notamment les standards en cours d'élaboration : "GPRS", "UTMS", etc. De façon générale, l'invention trouve application à chaque fois que l'on utilise un équipement mobile coopérant avec une carte à puce ou tout système  
30 embarqué similaire, et qu'il existe une séparation entre des fonctions directement implantées dans ce système embarqué et des fonctions présentes dans l'équipement mobile.



- Elle permet aussi un interfaçage avec des applications de type "WAP" ou de réaliser des fonctions de ce type. Par exemple, une application maître, présente sur un serveur éloigné, peut directement accéder au réseau Internet, à la demande de l'équipement mobile, sans repasser au préalable par l'équipement mobile. Le résultat des requêtes posées est ensuite renvoyé à l'application esclave, selon le processus propre à l'invention.
- 5

## REVENDEICATIONS

1. Procédé de transmission et de traitement de données numériques sur un réseau de téléphonie mobile, ledit réseau comprenant au moins un équipement mobile et un serveur éloigné comprenant des moyens de traitement d'information et de stockage de données, communiquant entre eux via ledit réseau de téléphonie mobile, ledit équipement mobile coopérant avec un système embarqué à puce électronique comprenant des moyens de traitement d'information et de stockage de données destinés à mémoriser au moins des pièces de logiciel d'un type capable, tout à la fois, de commander ledit équipement mobile par l'émission de commandes déterminées et de réagir à des événements provenant de cet équipement par exécution d'instructions associées à ces dits événements, en vue de réaliser des fonctionnalités associées à au moins une application prédéterminée, caractérisé en ce qu'il comprend l'implémentation d'au moins une première pièce de logiciel particulière (21), d'un type dit rapporteur, stockée dans lesdits moyens de stockage de données dudit système embarqué à puce électronique (2 - 20), et l'implémentation d'au moins une pièce de logiciel associée (30M) stockée dans lesdits moyens de stockage de données de l'un desdits serveurs éloignés (3), en ce que ladite pièce de logiciel de type rapporteur (21) retransmet à ladite pièce de logiciel associée (30M) des données caractéristiques desdits événements reçus dudit équipement mobile (1 - 10) et en ce que cette pièce de logiciel associée (30M) exécute, par l'intermédiaire desdits moyens de traitement d'information dudit serveur éloigné (3), sur réception desdites données caractéristiques, tout ou partie desdites instructions associées à l'une desdites applications prédéterminées et retransmet des résultats de ladite exécution au dit équipement mobile (1 - 10) et/ou au dit système embarqué à puce électronique (2 - 20).

2. Procédé selon la revendication 1, caractérisé en ce que ledit système embarqué à puce électronique (2 - 20) étant sous la commande d'un système d'exploitation déterminé, ladite pièce de logiciel associée (30M) implémentée sur un desdits serveurs éloignés (3) transmet lesdits résultats d'exécution sous forme de commandes envoyées directement au dit système d'exploitation pour réaliser une opération déterminée et en ce que des résultats de cette opération sont retransmis à ladite pièce de logiciel associée (30M).
3. Procédé selon la revendication 1, caractérisé en ce que, lesdites pièces de logiciel associées (30M) implémentées sur lesdits serveurs éloignés (3) étant d'un type dit maître, il comprend l'implémentation d'au moins une deuxième pièce de logiciel particulière (22), type dit esclave, stockée dans lesdits moyens de stockage dudit système embarqué à puce électronique (2 - 20), en ce que chacune desdites pièces de logiciel de type esclave (22) reçoit des commandes d'une desdites pièces de logiciel de type maître (30M), qui lui est associée, et exécute lesdites commandes par l'intermédiaire desdits moyens de traitement d'information dudit système embarqué à puce électronique (2 - 20), et en ce que ladite pièce de logiciel de type esclave (22) retransmet des résultats de ladite exécution de commandes à ladite pièce de logiciel de type maître associée (30M).
4. Procédé selon la revendication 3, caractérisé en ce que lesdites pièces de logiciel de types rapporteur (21) et/ou esclave (22) sont associées à une fonctionnalité supplémentaire, d'un type dit autonome, de manière à ce que ces pièces de logiciel (21, 22) puissent exécuter directement sur ledit système embarqué à puce électronique (2 - 20) une partie préétablie desdites applications prédéterminées.
5. Procédé selon la revendication 4, caractérisé en ce que ledit réseau de téléphonie mobile obéit à la norme dite "GSM" et lesdites pièces de logiciel obéissent à la norme "GSM 11.14".

6. Procédé selon la revendication 1, caractérisé en ce que, ledit réseau de téléphonie comprenant au moins deux canaux de transmission distincts, un canal dit de données de voix et un canal dit de messages, lesdites données numériques transmises sont constituées de messages d'un type dit court comprenant 140 octets ou 160 septets transmis par ledit canal de messages.
7. Système embarqué équipé d'une puce électronique comprenant des moyens de traitement d'information et de stockage de données destinés à mémoriser au moins des pièces de logiciel du type capable, tout à la fois, de commander ledit équipement mobile par l'émission de commandes déterminées et de réagir à des événements provenant de cet équipement par exécution d'instructions associées à ces dits événements, en vue de réaliser des fonctionnalités associées à au moins une application prédéterminée, ledit système embarqué à puce électronique coopérant avec un équipement mobile relié à un réseau de téléphonie mobile, ledit réseau de téléphonie mobile étant connecté avec au moins un serveur éloigné comprenant des moyens de traitement d'information et de stockage de données communiquant avec ledit équipement mobile via ledit réseau de téléphonie mobile, caractérisé en ce que ledit système embarqué à puce électronique (2 -20) stocke dans ses dits moyens de stockage de données au moins une première pièce de logiciel particulière (21), d'un type dit rapporteur, destinée à retransmettre à une pièce de logiciel associée (30M), stockée dans lesdits moyens de stockage de données de l'un desdits serveurs éloignés (3), qui lui est associée, des données caractéristiques desdits événements reçus dudit équipement mobile (1 – 10 ), de manière à ce que cette pièce de logiciel associée (30M) exécute, par l'intermédiaire desdits moyens de traitement d'information dudit serveur éloigné (3), sur réception desdites données caractéristiques, tout ou partie desdites instructions associées à l'une desdites applications prédéterminées et retransmettre des résultats de ladite exécution au dit équipement mobile (1 – 10) et/ou au dit système embarqué à puce électronique (2 – 20).

8. Système embarqué à puce électronique selon la revendication 7, caractérisé en ce que lesdites pièces de logiciel associées (30M) implémentées sur lesdits serveurs éloignés (3) étant d'un type dit maître, il stocke dans ses dits moyens de stockage de données au moins une  
5 deuxième pièce de logiciel particulière (22), d'un type dit esclave, destinée à recevoir des commandes d'une desdites pièces de logiciel de type maître (30M), qui lui est associée, à exécuter lesdites commandes par l'intermédiaire desdits moyens de traitement d'information dudit système embarqué à puce électronique (2 – 20), et à retransmettre des  
10 résultats de ladite exécution de commandes à ladite pièce de logiciel de type maître associée (30M).
9. Système embarqué à puce électronique selon la revendication 8, caractérisé en ce que lesdites pièces de logiciel de types rapporteur (21) et/ou esclave (22) sont associées à une fonctionnalité supplémentaire,  
15 dite autonome, de manière à ce que ces pièces de logiciel puissent exécuter directement sur ledit système embarqué à puce électronique (2 – 20) une partie préétablie desdites applications prédéterminées.
10. Système embarqué à puce électronique caractérisé en ce qu'il est constitué par une carte à puce du type dit "SIM" (2).

**REVENDEICATIONS**

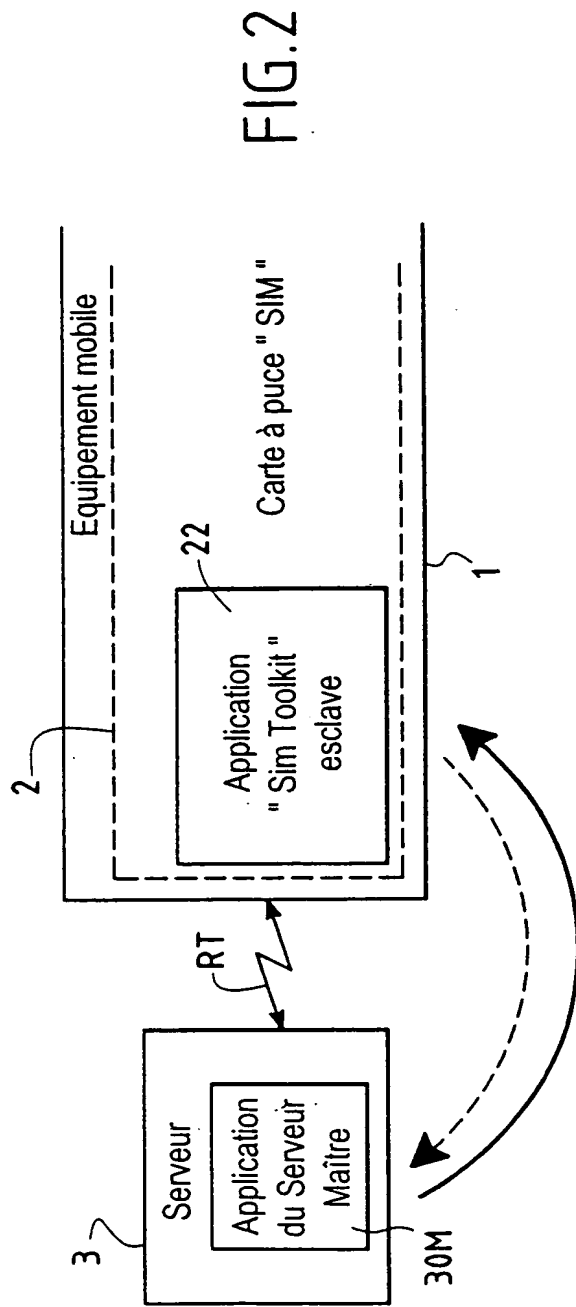
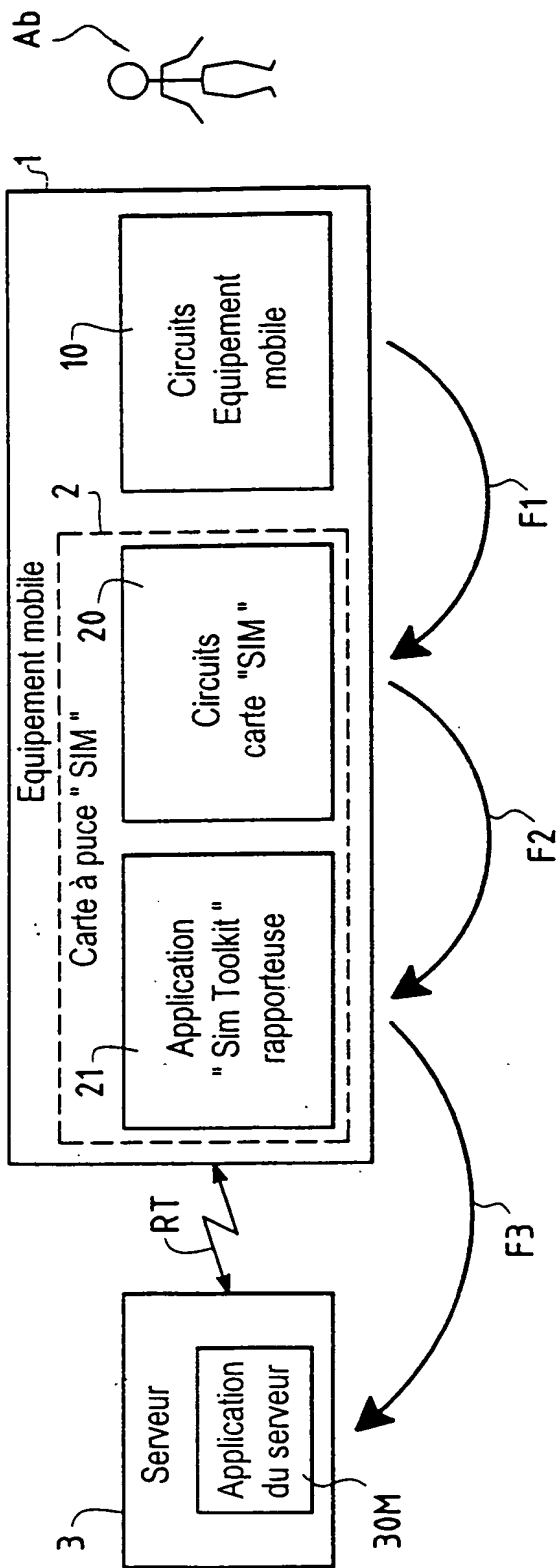
1. Procédé de transmission et de traitement de données numériques sur un réseau de téléphonie mobile comprenant un équipement mobile coopérant avec un système embarqué (2 - 20) muni de moyens de traitement d'information et de stockage de données, caractérisé en ce qu'il consiste au moyen d'au moins  
5 une première pièce de logiciel particulière (21), d'un type dit rapporteur, stockée dans lesdits moyens de stockage de données dudit système embarqué (2 - 20), à déléguer l'exécution de traitement s'effectuant dans ledit système embarqué en réponse à au moins un événement reçu dudit équipement mobile, à au moins une pièce de logiciel associée (30M) stockée dans des moyens de  
10 stockage de données d'au moins un serveur éloigné (3).
2. Procédé selon la revendication 1, caractérisée en ce que les moyens de traitement d'information et de stockage de données dudit système embarqué sont destinés à mémoriser au moins des pièces de logiciel d'un type capable, tout à la fois, de commander ledit équipement mobile par l'émission de  
15 commandes déterminées et de réagir à des événements provenant de cet équipement par exécution d'instructions associées à ces dits événements, en vue de réaliser des fonctionnalités associées à au moins une application prédéterminée.
3. Procédé selon l'une des revendications précédentes, caractérisé en ce ladite  
20 (ou lesdites) pièce de logiciel de type rapporteur (21) retransmet à ladite (ou lesdites) pièce de logiciel associée (30M) des données caractéristiques desdits événements reçus dudit équipement mobile (1 - 10) et en ce que cette pièce de logiciel associée (30M) exécute, par l'intermédiaire de moyens de traitement d'information dudit serveur éloigné (3), sur réception desdites données  
25 caractéristiques, tout ou partie desdites instructions associées à l'une desdites applications prédéterminées et retransmet des résultats de ladite exécution au dit équipement mobile (1 - 10) et/ou au dit système embarqué à puce électronique (2 - 20).

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que ledit système embarqué (2 - 20) étant sous la commande d'un système d'exploitation déterminé, ladite (ou lesdites) pièce de logiciel associée (30M) implémentée sur un desdits serveurs éloignés (3) transmet lesdits résultats d'exécution sous forme de commandes envoyées directement au dit système d'exploitation pour réaliser une opération déterminée et en ce que des résultats de cette opération sont retransmis à ladite pièce de logiciel associée (30M).
5. Procédé selon l'une des revendications précédentes, caractérisé en ce que, ladite (ou lesdites) pièce de logiciel associée (30M) implémentée sur lesdits serveurs éloignés (3) étant d'un type dit maître, il comprend l'implémentation d'au moins une deuxième pièce de logiciel particulière (22), type dit esclave, stockée dans lesdits moyens de stockage dudit système embarqué (2 - 20), en ce que chacune desdites pièces de logiciel de type esclave (22) reçoit des commandes d'une desdites pièces de logiciel de type maître (30M), qui lui est associée, et exécute lesdites commandes par l'intermédiaire desdits moyens de traitement d'information dudit système embarqué (2 - 20), et en ce que ladite pièce de logiciel de type esclave (22) retransmet des résultats de ladite exécution de commandes à ladite pièce de logiciel de type maître associée (30M).
6. Procédé selon la revendication 5, caractérisé en ce que lesdites pièces de logiciel de types rapporteur (21) et/ou esclave (22) sont associées à une fonctionnalité supplémentaire, d'un type dit autonome, de manière à ce que ces pièces de logiciel (21, 22) puissent exécuter directement sur ledit système embarqué à puce électronique (2 - 20) une partie préétablie desdites applications prédéterminées.
7. Procédé selon l'une des revendications précédentes, caractérisé en ce que ledit réseau de téléphonie mobile obéit à la norme dite "GSM" et lesdites pièces de logiciel obéissent à la norme "GSM 11.14".
8. Procédé selon l'une des revendications précédentes, caractérisé en ce que, ledit réseau de téléphonie comprenant au moins deux canaux de transmission

distincts, un canal dit de données de voix et un canal dit de messages, lesdites données numériques transmises sont constituées de messages d'un type dit court comprenant 140 octets ou 160 septets transmis par ledit canal de messages.

- 5 **9.** Système embarqué comprenant des moyens de traitement d'information et de stockage de données, ledit système embarqué étant destiné à coopérer avec un équipement mobile caractérisé en ce qu'il comprend au moins une première pièce de logiciel particulière (21), d'un type dit rapporteur, stockée dans lesdits moyens de stockage de données dudit système embarqué (2 - 20) destinée à
- 10 déléguer l'exécution de traitement s'effectuant dans ledit système embarqué en réponse à au moins un événement reçu dudit équipement mobile, à au moins une pièce de logiciel associée (30M) stockée dans des moyens de stockage de données d'au moins un serveur éloigné (3).
- 10.** Système embarqué selon la revendication 9, caractérisé en ce que ladite (ou
- 15 lesdites) pièce de logiciel associée (30M) implémentée sur ledit (ou lesdits) serveur éloigné (3) étant d'un type dit maître, il stocke dans ses dits moyens de stockage de données au moins une deuxième pièce de logiciel particulière (22), d'un type dit esclave, destinée à recevoir des commandes d'une desdites pièces de logiciel de type maître (30M), qui lui est associée, à exécuter lesdites
- 20 commandes par l'intermédiaire desdits moyens de traitement d'information dudit système embarqué (2 - 20), et à retransmettre des résultats de ladite exécution de commandes à ladite pièce de logiciel de type maître associée (30M).
- 11.** Système embarqué selon l'une des revendications 9 ou 10, caractérisé en ce que lesdites pièces de logiciel de types rapporteur (21) et/ou esclave (22) sont
- 25 associées à une fonctionnalité supplémentaire, dite autonome, de manière à ce que ces pièces de logiciel puissent exécuter directement sur ledit système embarqué (2 - 20) une partie préétablie desdites applications prédéterminées.
- 12.** Système embarqué selon l'une des revendications 9 à 11, caractérisé en ce qu'il est constitué par une carte à puce du type dit "SIM" (2).





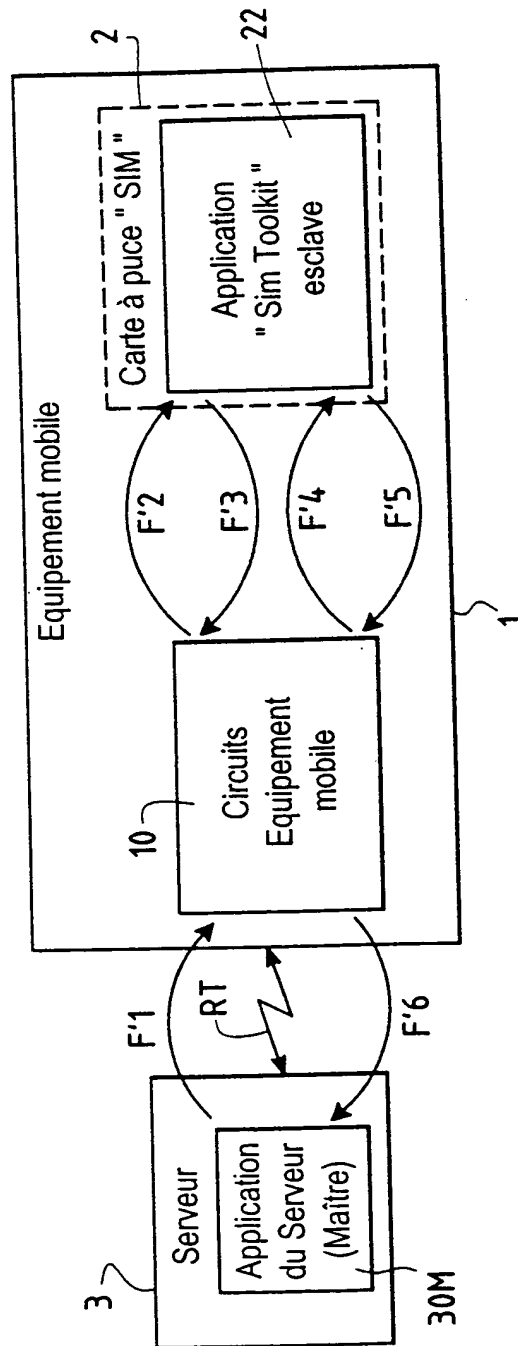
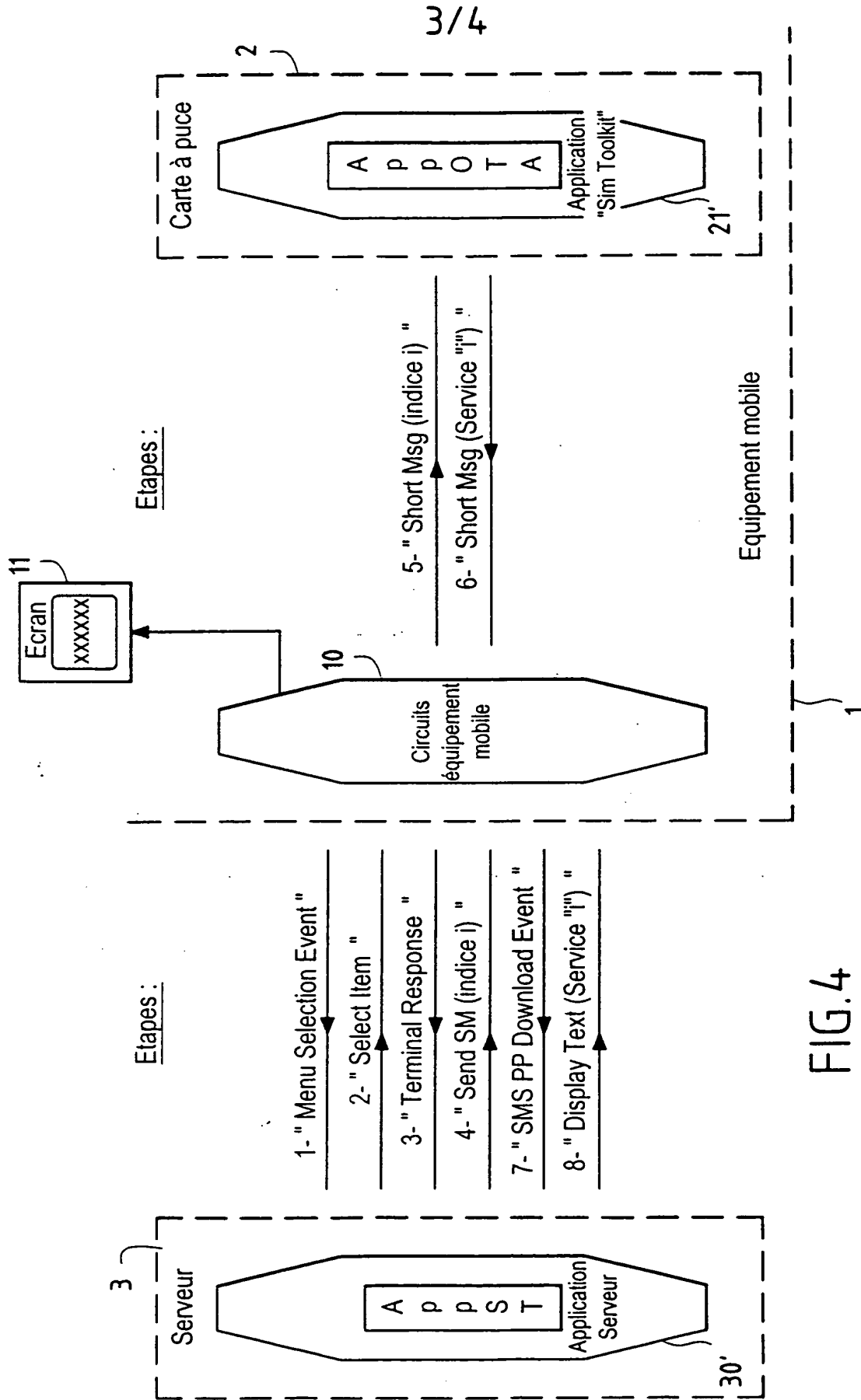


FIG.3



**FIG.4**  
ART ANTERIEUR

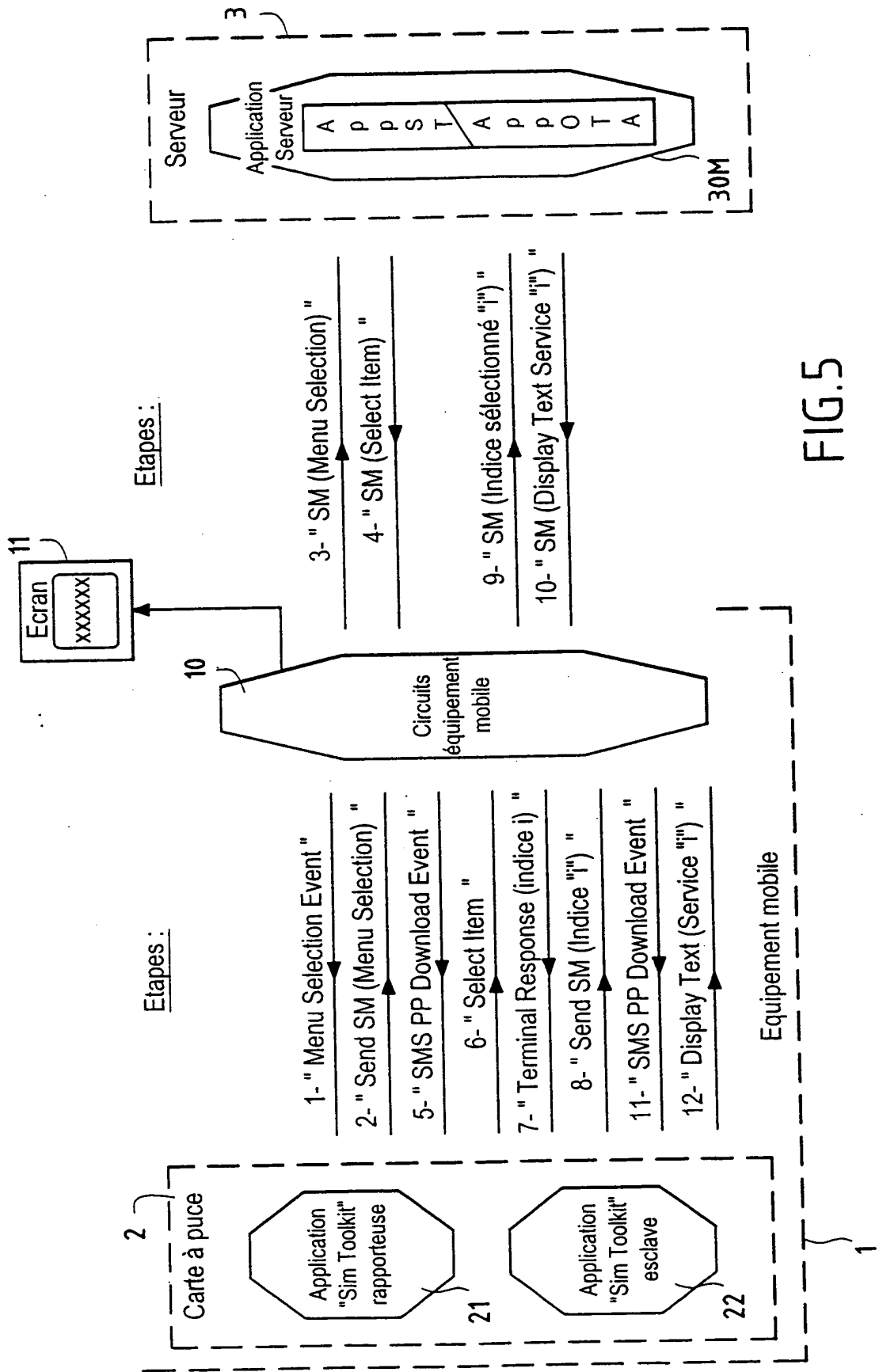


FIG.5

FRENCH REPUBLIC

**INPI**

NATIONAL  
INSTITUTE OF  
INDUSTRIAL  
PROPERTY

---

**PATENT**

---

**CERTIFICATE OF UTILITY – CERTIFICATE OF ADDITION**

**OFFICIAL COPY**

The Director General of the National Institute of Industrial Property certifies that the attached document is a certified copy of an application for title to industrial property filed at the Institute.

**Issued in Paris      05 DEC 2005**

**For the Director General of the  
National Institute of Industrial Property  
Patent Division Director**

**[SIGNED]**

**Martine PLANCHE**

**NATIONAL  
INSTITUTE OF  
INDUSTRIAL  
PROPERTY**

**HEAD OFFICE**  
26 bis ,rue de Saint Pétersbourg  
75800 PARIS cedex 08  
Telephone: 33 (0)1 53 04 53 04  
Fax: 33 (0)1 53 04 45 23  
[www.inpi.fr](http://www.inpi.fr)

**THIS PAGE BLANK (USPTO)**

**INPI**

National Institute  
Of Industrial Property  
26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Telephone: 01 53 04 53 04 Fax: 01 42 94 86 54

# **PATENT OF INVENTION CERTIFICATE OF UTILITY**

Intellectual Property Code – Book VI

## **REQUEST FOR ISSUE 1/2**

This form must be filled in legibly in black ink.

<i>Reserved for INPI use</i> DELIVERY OF DOCUMENTS DATE <b>22 JUNE 2000</b> LOCATION <b>75 INPI PARIS</b> NATIONAL REGISTRATION NO. ASSIGNED BY THE INPI <b>0007978</b> FILING DATE ASSIGNED BY THE INPI <b>22 JUNE 2000</b> Your references for this file (optional) <b>FR 3882/BC</b>		<b>1</b> NAME AND ADDRESS OF APPLICANT OR AGENT TO WHOM CORRESPONDENCE SHOULD BE ADDRESSED  <b>BULL S.A.</b> <b>CORLU Bernard – PC/58D20</b> <b>68, route de Versailles</b>  <b>78434 LOUVECIENNES Cedex</b>	
Confirmation of a filing by facsimile <input type="checkbox"/> No. assigned to the facsimile by the INPI:			
<b>2 NATURE OF THE APPLICATION</b>		Check one of the following four boxes	
Patent application		<input checked="" type="checkbox"/>	
Application for certificate of utility		<input type="checkbox"/>	
Divisional application		<input type="checkbox"/>	
<i>Initial patent application</i> No. _____ Date ____ / ____ / ____			
<i>or initial certificate of utility application</i> No. _____ Date ____ / ____ / ____			
Transformation of a European patent application		<input type="checkbox"/>	
<i>Initial patent application</i> No. _____ Date ____ / ____ / ____			
<b>3 TITLE OF THE INVENTION (200 characters or spaces maximum)</b>  <b>METHOD FOR PROCESSING AND TRANSMITTING DIGITAL DATA IN A MOBILE TELEPHONE NETWORK, PARTICULARLY USING THE “GSM” STANDARD, AND EMBEDDED MICROCHIP SYSTEM</b>			
<b>4 PRIORITY DECLARATION OR REQUEST FOR BENEFIT OF THE FILING DATE OF A PRIOR FRENCH APPLICATION</b>		Country or organization Date ____ / ____ / ____ : No. _____ Country or organization Date ____ / ____ / ____ : No. _____ Country or organization: Date ____ / ____ / ____ : No. _____ <input type="checkbox"/> If there are other priorities, check this box and use the “Continued” form	
<b>5 APPLICANT</b>		<input type="checkbox"/> If there are other applicants, check this box and use the “Continued” form	
Last name or company name		<b>BULL CP8</b>	
First name			
Legal status		<b>Corporation</b>	
SIREN No.		<b>3 · 2 · 9 · 5 · 5 · 6 · 1 · 4 · 6</b>	
APE-NAF Code		<b>B · 3 · 2 · 1</b>	
Address	Street	<b>BP 45 – 68, route de Versailles</b>	
	Postal code and city	<b>78430</b>	<b>LOUVECIENNES</b>
Country		<b>France</b>	
Nationality		<b>French</b>	
Telephone number (optional)		<b>01.39.66.61.76</b>	
Fax number (optional)		<b>01.39.66.61.73</b>	
Email address (optional)		<b>BERNARD.CORLU@BULL.NET</b>	

THIS PAGE BLANK (USPTO)



**INPI**National Institute  
Of Industrial Property**PATENT OF INVENTION  
CERTIFICATE OF UTILITY**

REQUEST FOR ISSUE 2/2

<i>Reserved for INPI Use</i>	
DELIVERY OF DOCUMENTS	
DATE <b>22 JUNE 2000</b>	
LOCATION <b>75 INPI PARIS</b>	
NATIONAL REGISTRATION NO.	
ASSIGNED BY THE INPI <b>0007978</b>	
<b>Your references for this file:</b> <i>(optional)</i>	
<b>FR 3882/BC</b>	
<b>6 AGENT</b>	
Last name <b>CORLU</b>	
First name <b>Bernard</b>	
Firm or Company <b>BULL S.A.</b>	
Permanent proxy no. and/or contractual relationship <b>PG 4280</b>	
Address	Street <b>68, route de Versailles / PC 58D20</b>
	Postal code and city <b>78434 LOUVECIENNES CEDEX</b>
Telephone no. <i>(optional)</i> <b>01.39.66.61.76</b>	
Fax no. <i>(optional)</i> <b>01.39.66.61.73</b>	
Email address <i>(optional)</i> <b>BERNARD.CORLU@BULL.NET</b>	
<b>7 INVENTOR(S)</b>	
The inventors are the applicants <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <b>In this case provide a separate Designation of Inventor(s)</b>	
<b>8 SEARCH REPORT</b>	
<b>For patent applications only (including division and transformation)</b>	
Immediate preparation or deferred preparation <input checked="" type="checkbox"/> Immediate <input type="checkbox"/> Deferred	
Payment of fee in installments <b>Payment in three installments, for natural persons only</b> <input type="checkbox"/> Yes <input type="checkbox"/> No	
<b>9 FEE DISCOUNT</b>	
<b>For natural persons only</b> <input type="checkbox"/> Requested for the first time for this invention <i>(attach certificate of non-assessment)</i> <input type="checkbox"/> Requested prior to this filing <i>(attach a copy of the acceptance ruling for this invention or indicate its reference.)</i>	
If you have used the "Continued" form, indicate the number of pages attached <b>0</b>	
<b>10 SIGNATURE OF APPLICANT OR AGENT</b> (Name and title of signatory)	
<b>[SIGNED]</b>  <b>CORLU Bernard</b> (Agent)	
<b>STAMP OF THE AUTHORITY OR THE INPI</b>  <b>H. ADAO</b> <b>[STAMP]</b>	

Law No. 78-17 of January 6, 1978 relative to data processing, files and rights applies to the responses entered on this form.  
It guarantees the right to access and correct any data at the INPI that concern you.

**THIS PAGE BLANK (USPTO)**

**INPI**National Institute  
Of Industrial Property

PATENT DEPARTMENT

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Telephone: 01 53 04 53 04 Fax: 01 42 94 86 54**PATENT OF INVENTION**  
**CERTIFICATE OF UTILITY**  
Intellectual Property Code – Book VI**DESIGNATION OF INVENTOR(S) Page No. 1 / 1**  
(If the applicant is not the inventor or the sole inventor)

This form must be filled in legibly in black ink.

<b>Your references for this file</b> (optional)		<b>FR 3882/BC</b>	
<b>NATIONAL REGISTRATION NO.</b>		<b>0007978</b>	
<b>TITLE OF THE INVENTION (200 characters or spaces maximum)</b>  <b>METHOD FOR PROCESSING AND TRANSMITTING DIGITAL DATA IN A MOBILE TELEPHONE NETWORK, PARTICULARLY USING THE "GSM" STANDARD, AND EMBEDDED MICROCHIP SYSTEM</b>			
<b>THE APPLICANT(S)</b>  <b>BULL CP8</b> <b>BP 45 – 68, route de Versailles</b> <b>78430 LOUVECIENNES – FRANCE</b>			
<b>DESIGNATE(S) AS THE INVENTOR(S):</b> (Indicate at top right "Page No. 1/1." If there are more than three inventors, use an identical form and number each page indicating the total number of pages).			
Last name		<b>NACHEF</b>	
First Name		<b>Armand</b>	
Address	Street	<b>21 boulevard Vauban</b>	
	Postal code and city	<b>78180</b>	<b>Montigny le Bretonneux – FRANCE</b>
Company of affiliation (optional)			
Last name			
First Name			
Address	Street		
	Postal code and city		
Company of affiliation (optional)			
Last name			
First Name			
Address	Street		
	Postal code and city		
Company of affiliation (optional)			
<b>DATE AND SIGNATURE(S)</b> <b>OF THE APPLICANT(S)</b> <b>OR AGENT</b> (Name and title of signatory)		<b>Louveciennes, June 20, 2000</b>  <b>[SIGNED]</b> <b>CORLU, Bernard (Agent)</b>	

Law No. 78-17 of January 6, 1978 relative to data processing, files and rights applies to the responses entered on this form.  
It guarantees the right to access and correct the data at the INPI that concern you.

**THIS PAGE BLANK (USPTO)**

## DOCUMENT COMPRISING MODIFICATIONS

PAGE(S) OF THE SPECIFICATION, THE CLAIMS OR THE DRAWINGS			A.C.*	DATE OF LETTER	EXAMINER'S DATE STAMP
Amended	Deleted	Added			
<i>26 through 28</i>	<i>29</i>		<i>X</i>	<i>10/15/01</i>	<b>08 APR 2005/TFA</b>

Any change made to the wording of the original claims, unless it follows from the provisions of Article R.612-36 of the Intellectual Property Code, is indicated by the notation "A.C." (amended claims).

**THIS PAGE BLANK (USPTO)**

The invention relates to a method for processing and transmitting digital data in a mobile telephone network.

It applies more particularly to a mobile telephone network that complies with the "GSM" standard (the acronym for Global System for Mobile Communication, operating in the 900 MHz bandwidth).

The invention also relates to an embedded system equipped with a microchip for implementing the method.

Within the scope of the invention, the term "network" should be understood in its most general sense. It includes the transmission components of the network *per se* (radio transmission subsystems, transmission cables, hertzian waves, "wired" ground subsystems, etc.), but also all the systems connected to the mobile telephone network (base stations, station controllers, switching systems, directories, etc., and more generally, all data processing systems and servers connected to the network), including the mobile telephones, equipment, or stations carried by the users (subscribers) of the mobile telephone network.

The latter devices can be portable telephones or more complex terminals, for example a terminal that combines the telephone and organizer functionalities. For simplicity's sake, without in any way limiting the scope of the invention, these devices will hereinafter be called "mobile telephones." The mobile telephones are specifically equipped with an embedded system equipped with data processing and storage means, including a functional module known by the abbreviation "SIM" (for "Subscriber Identity Module"). Also for simplicity's sake, it will be assumed hereinafter that the "SIM" module is installed in a smart card. Software for operating the smart card is also provided (called "OS," for "Operating System").

In the current state of the art, the mobile telephones of GSM networks are no longer used just for telephoning. They can also be used to process and send digital data, particularly in the form of short messages (a service called "GSM-Data"). These messages typically have a length of 160 septets or 140 octets, depending on the application.

Recently, we have seen the appearance of a standardized technology called "SIM Toolkit." This technology is already included in the supplementary services offered by certain mobile telephone operators of GSM networks. In a practical way, a specific piece of software is implemented in the "SIM" smart card of the telephone.

**THIS PAGE BLANK (USPTO)**



This standard allows the applications running in the smart card ("SIM") of the mobile telephone to send commands to the associated mobile equipment for:

- . displaying a text on the screen of the mobile telephone;
- . prompting the user to type text as input into the application;
- . requesting a telephone call to a number;
- . requesting the sending of a short message that contains text or data to a server or to another telephone;
- . requesting the execution of a command in an auxiliary smart card in the mobile equipment;
- . etc.

These commands are called "proactive" commands.

The "SIM Toolkit" standard also allows the applications of the "SIM" smart card to react upon reception of a certain number of events originating from the mobile equipment. These events include:

- . the selection of the application from a so-called "MENU" command located on a keyboard with which the mobile equipment is equipped;
- . the reception of a short message sent to an application or to the operating system of the "SIM" smart card;
- . the expiration of the time programmed into a timer of the mobile equipment;
- . a request to call a telephone number;
- . etc.

The functionalities provided by this standard make it possible to develop a very large number of distinct applications in the smart card, in order to provide users with so-called "value-added" services.

For a more detailed description of "SIM Toolkit" technology, it would be useful to refer to the GSM 11.14 standard.

In summary, in the current state of the art, the "SIM Toolkit" standard consists of developing applications in the smart card that are capable both of controlling the mobile equipment supporting the smart card and of reacting to events originating from this equipment. Today, this standard has been adopted by the majority of manufacturers of mobile equipment and smart cards. It is a standard that makes it possible to write applications that are both powerful and secure.

**THIS PAGE BLANK (USPTO)**

A "SIM Toolkit" application generally communicates with one or more applications installed in servers, via the short message channel. This channel is independent from the voice channel and is standardized by the GSM standard. The applications, whether they are installed in the SIM card or in the server, can both send and receive short messages that contain text or data in binary format. (For more information on short messages in point-to-point mode, see the GSM 03.40 standard.)

However, while the number and nature of the aforementioned value-added GSM services are *a priori* unlimited, telephone operators and developers of software applications are constantly held back by the limited resources available in the smart card.

In essence, the two main drawbacks of the "SIM Toolkit" technology are;

1) insufficient memory in the smart cards for hosting "SIM Toolkit" applications, since they include only several tens of kilobytes of memory; in spite of all the optimizations provided by highly experienced developers of software applications, telephone service operators run up against this lack of memory for loading and/or running large numbers of "SIM Toolkit" applications; and

2) the long response time of smart cards; in essence, this technology requires the smart card, which is equipped with minimal computing power compared to the processors of mobile equipment, and especially servers, to perform the most complicated calculations during the execution of the aforementioned applications.

It is clear that the needs that have arisen run in the opposite direction. First of all, telephone operators want to offer their subscribers the largest possible number of available additional services. Moreover, the operations performed by the smart card must be executed in a minimal amount of time. The increase in available applications, to the extent that this increase is possible, also runs the risk of degrading performance by making the processing time even longer, due to mutual interactions.

Despite the substantial advances in smart card technology already seen in recent periods and foreseeable in the near future, the aforementioned limiting factors remain and will remain a significant obstacle.

A second standardized technology called "WAP" (for "Wireless Application Protocol") has recently been proposed. The purpose of this standard is to allow users of mobile telephones to access the Internet from their mobile telephones, via a wireless link.

This technology is not without drawbacks.

**THIS PAGE BLANK (USPTO)**

First of all, it is necessary to install a "WAP" browser of a specific type, since it has different characteristics than conventional Web browsers. This browser is installed in the mobile equipment, which definitely has more memory than the smart card, but generally less than a microcomputer and naturally less than a server. Furthermore, although this technology offers the advantage of allowing access to the Internet, it does not cover all the functionalities of SIM Toolkit applications. To give a nonlimiting example, a WAP application cannot, as in the case of SIM Toolkit applications, place telephone calls. Moreover, a WAP application cannot guarantee the same degree of security as that offered by SIM Toolkit applications. In essence, the latter use secret keys stored in the SIM smart cards. For example, a WAP application cannot request the authentication of an application in any server. Moreover, this is not the only security function devolved to the SIM smart card. It also ensures the security and confidentiality of the transmitted information.

In order to provide all of these functions, the smart card stores a certain amount of so-called "sensitive" data, encryption algorithms and associated keys, including:

- the international subscriber number of "IMSI" (for "International Mobile Subscriber Identity");
- the temporary identity assigned to a mobile station when it moves or "TMSI" (for "Temporary Mobile Subscriber Identity");
- an individual authentication key, an encryption key used to encrypt and decrypt so-called signaling and traffic data on the radio channel and three distinct encryption and decryption or key generating algorithms; and
- a number of encryption key sequences or "CKSN" (for "Ciphering Key Sequential Number") indicating the above valid encryption value, in order to avoid the use of different keys by the mobile station and the network.

The fact that this sensitive information or data is stored in the smart card and that the corresponding operations are performed in it makes it possible to obtain a high degree of security and confidentiality.

Finally, in the current state of the art, the cost of mobile equipment that supports WAP technology is still high compared to the cost of equipment that supports SIM Toolkit technology.

**THIS PAGE BLANK (USPTO)**

The invention seeks to eliminate the drawbacks of the devices and systems of the prior art, some of which have been summarized, while meeting the needs that continue to arise.

The object of the invention is a method for processing and transmitting digital data in a mobile telephone network, particularly using the GSM standard, that makes it possible to offer the users of mobile telephones in this network all of the services that can be offered with applications compliant with SIM Toolkit technology, while eliminating the limitations on memory and performance encountered in the development of applications in smart cards, at least most of them.

To do this, the invention advantageously uses the fact that applications compliant with SIM Toolkit technology can specifically send short messages and can also handle the execution of instructions upon reception of other short messages that are sent to them.

The mobile telephone network architecture according to the invention is an architecture in which SIM Toolkit applications:

- 1) inform applications installed in at least one remote server connected to said telephone network of the arrival of events originating from a unit of mobile equipment; these applications will hereinafter be called "reporter SIM Toolkit applications"; and

- 2) execute commands and instructions in response to requests for applications implemented in said servers; these applications will hereinafter be called "slave SIM Toolkit applications.

This way, it is possible to delegate the execution of intensive operations that use a lot of computer resources, which in the prior art is performed in the SIM smart card, to applications implemented in these servers.

The aforementioned servers do not *a priori* have any intrinsic limitations as do the SIM smart cards, either in terms of the quantity of available memory or in terms of computing power. The number of SIM Toolkit applications available via a SIM smart card (and hence the number of services offered) can therefore be greatly increased, while allowing a high processing speed.

Furthermore, since the functionalities linked to security and confidentiality remain confined in the SIM smart card, as in the prior art, a high level of quality of service continues to be guaranteed.

**THIS PAGE BLANK (USPTO)**



Hence, the main subject of the invention is a method for transmitting and processing digital data in a mobile telephone network, said network comprising at least one unit of mobile equipment and a remote server comprising information processing and data storage means communicating with one another via said mobile telephone network, said mobile equipment cooperating with an embedded microchip system comprising information processing and data storage means for storing at least certain pieces of software capable both of controlling said mobile equipment by sending given commands and of reacting to events originating from this equipment by executing instructions associated with said events, in order to perform functionalities associated with at least one predetermined application, characterized in that it includes the implementation of at least a first particular piece of software of a so-called reporter type, stored in said data storage means of said embedded microchip system, and the implementation of at least one associated piece of software stored in said data storage means of one of said remote servers, in that said piece of software of the reporter type retransmits to said associated piece of software data characteristic of said events received from said mobile equipment and in that said associated piece of software executes, using said information processing means of said remote server, upon reception of said characteristic data, all or some of said instructions associated with one of said predetermined applications and retransmits results of said execution to said mobile equipment and/or to said embedded microchip system.

Another subject of the invention is an embedded system equipped with a microchip cooperating with a unit of mobile equipment connected to said mobile telephone network.

The invention will now be described in greater detail by referring to the attached drawings, in which:

- Fig. 1 is a diagram that schematically illustrates the main steps of the activation of a SIM Toolkit application located in a remote server by an application according to one aspect of the invention of a first so-called "reporter" type, located in a SIM smart card;

- Fig. 2 is a diagram that schematically illustrates the interrelation according to the invention between an application located in a remote server, of a so-called "master" type, and a SIM Toolkit application located in a SIM smart card, of a second so-called "slave" type, according to another aspect of the invention;

**THIS PAGE BLANK (USPTO)**

- Fig. 3 is a diagram illustrating the main steps of the method according to the invention for sending a proactive command according to the GSM 11.14 standard;

- Fig. 4 is a diagram illustrating, for one particular example, the main steps for exchanging data and commands between a SIM Toolkit application located in a SIM smart card and an application located in a remote server, according to the prior art; and

- Fig. 5 is a diagram illustrating, for this particular example, the main steps for exchanging data and commands between a SIM Toolkit application located in a SIM smart card and an application located in a remote server, according to the method of the invention.

We will now describe in greater detail a preferred exemplary embodiment of a mobile telephone network architecture according to the invention.

As indicated above, according to one of the characteristics of the invention, the execution of intensive operations, which in the prior art is performed in the SIM card, is delegated to applications implemented in one or more remote servers connected to the network.

According to another characteristic of the invention, two main categories of SIM Toolkit applications are provided, which will be called "Reporter SIM Toolkit Applications" and "Slave SIM Toolkit Applications," respectively, both implemented in the SIM smart cards.

We will now describe both types of applications in greater detail.

#### Reporter SIM Toolkit application

First of all, a SIM Toolkit application reacts to events originating from the mobile telephone, or more generally from the subscriber's mobile equipment. These events arrive in the SIM smart card in a command known as an "Envelope." The "Envelope" command can contain, for example, the "Menu Selection" event, with the selection subscript being that of this SIM Toolkit application. This event therefore makes it possible to choose an application from a menu that is displayed on display means with which the mobile telephone is equipped. A more detailed description of this command can be found in the GSM 11.14 standard.

The mobile equipment has no knowledge of the applications located in the servers. In order to make an application in a server react to events defined in the SIM

**THIS PAGE BLANK (USPTO)**

Toolkit standard, it is necessary to couple it with a SIM Toolkit application installed in the SIM card, which will hereinafter be called the "Reporter SIM Toolkit application." The mobile equipment sees the reporter application as though it were a conventional SIM Toolkit application. It has no knowledge of the corresponding application located in a server. From this point of view, there is total transparency.

The reporter application is written into the SIM Card in order to listen for events to which its corresponding application implemented in a server must react. As soon as the reporter application receives an event coming from the mobile equipment, it prepares a short message to be sent to its corresponding application. This short message contains all of the data that characterizes the event received. It is sent in a practical way by a command of the aforementioned "proactive command" type.

The corresponding application of the server receives the short message. This message informs it of the occurrence of an event coming from the mobile equipment. It then performs the operation related to the reception of this event. This operation can consist, for example, of connecting to a web site. It can also become a so-called master application of another so-called slave application implemented in the SIM smart card. It can consequently control the slave application so that it sends proactive commands to the mobile equipment and so that it also invokes methods stored in libraries installed in the SIM smart card.

Fig. 1 is a diagram that schematically illustrates the main steps in the activation of a SIM Toolkit application 30M located in a remote server 3 by an application of the "Reporter SIM Toolkit" 21 located in a SIM smart card 2 of a unit of mobile equipment 1. The remote server 3 and the mobile equipment 1 of the subscriber *Ab* are both connected to a mobile telephone network *RT* (not explicitly represented). This network, which is well known to one skilled in the art and intrinsically conventional, does not require any modification due to the method of the invention. It follows that, *a priori*, any network according to the prior art is usable, which represents an additional advantage of the invention. It is not necessary to further describe such a network and its various components. It may be useful, as a non-limiting example, to refer to the article by Jean Cellmer entitled "Réseaux Cellulaires, Système GSM" appearing in "Techniques de l'Ingénieur," Volume TE 7364, November 1999, pages 1 through 23.

The mobile equipment 1, for example a portable telephone, includes the conventional electronic circuits (memories, processor, etc.) 10. The latter can be

**THIS PAGE BLANK (USPTO)**

coupled with a SIM smart card 2 by means of a reader (not represented). The SIM smart card 2 also includes electronic circuits 20, particularly a processor and storage means in which SIM Toolkit applications can be stored, which will be referred to as conventional (not represented) since they are intrinsically common to the prior art, as well as one or more reporter SIM Toolkit applications 21 according to one of the characteristics of the invention. In Fig. 1, in order to illustrate the process simply, only one application is represented, shown outside the circuits 20 of the SIM smart card 2. In reality, this application 21 is stored, like the conventional applications, in the storage means of the smart card 2.

The aforementioned steps are the following (symbolized by solid arrows in Fig. 1):

- F1) the circuits 10 of the mobile equipment 1 send a command of the "Envelope" type to the circuits 20 of the SIM smart card 2: this "Envelope" command contains one of the events provided in the aforementioned GSM 11.14 standard;
- F2) the circuits 20 of the SIM card 2 send this event to a reporter SIM Toolkit application 21 capable of responding to it; and
- F3) the reporter SIM Toolkit application 21 sends this same event, in a short message, to a corresponding application 30M located in the server 3 that will process it, via the network *RT*.

For reasons that will be explained below, the application 30M will be called the "master application."

#### Slave SIM Toolkit application

In an intrinsically known way, a SIM Toolkit application of the prior art can specifically:

- a) send proactive commands in accordance with the GSM 11.14 standard to the mobile equipment; it can, for example, ask the mobile equipment to display text;
- b) send commands in accordance with the aforementioned GSM 11.11 standard to the operating system of the SIM smart card, without passing through the mobile equipment; and
- c) request the execution of methods stored in libraries implemented in the SIM smart card; it can for example call a method of the SIM smart card in

**THIS PAGE BLANK (USPTO)**



order to request the encryption of a message by means of a secret key stored in this card.

According to an additional aspect of the invention, the applications implemented in the remote servers are equipped with these functionalities. It is thus possible to delegate to them the operation that, in the prior art, is performed using a conventional SIM Toolkit application implemented in the smart card.

In order for an application implemented in a remote server 3 to be able to perform these operations, it is necessary for it to be able to communicate with a SIM Toolkit application implemented in the SIM smart card 2. It then sends commands to the latter application, which executes them. Hereinafter, the applications implemented in the remote servers will be called "master applications" and the SIM Toolkit applications installed in the SIM smart card will be called "slave SIM Toolkit applications."

Fig. 2 is a diagram that schematically illustrates the interrelation between these two types of applications.

A "Master" application 30M sends a command (solid line in Fig. 2) to a slave SIM Toolkit application 22. The latter application executes the command, then responds to the "Master" application 30M by returning the result of the command (broken line) to it after processing.

We will now describe in detail how a "Master" application 30M can send commands of the aforementioned types a) through c).

#### Sending a proactive command in accordance with the GSM 11.14 standard

The main steps of the method according to the invention are explained below, in reference to the diagram of Fig. 3:

- a) a master application 30M prepares a proactive command to be executed by the circuits 10 of a unit of mobile equipment 1; it includes it in the data of a short message sent to a slave SIM Toolkit application 22 (via the circuits 10 of a unit of mobile equipment 1, in which the proactive command is executed) – the arrows F'1 and F'2 in Fig. 3;
- b) the slave SIM Toolkit application 22 analyzes the data of the short message received; it understands that the master application 30M is asking it to send the proactive command to the circuits 10 of its mobile equipment 1; it

**THIS PAGE BLANK (USPTO)**

therefore transfers this command to the mobile equipment 1 and puts itself on standby for a return response – the arrow F'3;

c) the circuits 10 of the mobile equipment 1 receive the proactive command; they execute it and send a response to the SIM card 2 in the form of a command commonly called a "Terminal Response – the arrow F'4 – which command contains the result of the execution of the proactive command by the circuits 10 of the mobile equipment 1 (for example, if the proactive command consists of asking to power up an auxiliary smart card, not represented, in the mobile equipment 1, the result sent in the "Terminal Response" command contains a byte string that is the response of a reset of the auxiliary card);

d) the slave SIM Toolkit application 22, which has been on standby since the sending of the proactive command, is released upon reception of the aforementioned "Terminal Response" command;

e) the slave SIM Toolkit application 22 prepares a short message containing the result of the proactive command it found in the "Terminal Response" command issued by the circuits 10 of the mobile equipment 1;

f) the slave SIM Toolkit application 22 sends this short message, in a proactive command, to the master application 30M, via the circuits 10 of the mobile equipment 1 – the arrow F'5;

g) the circuits 10 of the mobile equipment 1 transfer the short message to the master application 30M – the arrow F'6; and

h) the master application 30M receives it and processes the response to the proactive command it sent previously.

#### Sending a "non-proactive" command, i.e., in accordance with the GSM 11.11 standard

The master application 30M (Fig. 3) can send GSM 11.11 commands to the SIM smart card 2 using two different methods, either of which two methods can be used.

##### Method 1

a) a master application 30M prepares a command in accordance with the GSM 11.11 standard, to be sent to a slave SIM Toolkit application 22 implemented in the SIM smart card 2; it sends it in a short message, via the circuits 10 of the mobile equipment 1;

**THIS PAGE BLANK (USPTO)**

b) the slave SIM Toolkit application 22 analyzes the data of the short message received; it transmits the command found in this message to the operating system 23 of the SIM smart card 2;

c) the operating system 23 of the SIM smart card 2 executes the command that comes from the slave SIM Toolkit application 22 and returns a response to this command to this application 22;

d) the slave SIM Toolkit application 22 prepares a short message having as its destination a corresponding master application 30M implemented in the remote server 3; this message contains the result of the GSM 11.11 command and is sent by the slave application to the circuits 10 of the mobile equipment 1, in a proactive command;

e) the circuits 10 of the mobile equipment 1 transfer the short message to the address of the recipient indicated in the message itself, i.e., the master application 30M; and

f) the master application 30M receives it and processes the response received.

#### Method 2

The master application 30, implemented in the remote server 3, sends a GSM 11.11 command in a short message directly to the operating system 23 of the SIM smart card, in accordance with the GSM 03.40 and GSM 03.48 standards.

The advantage of this solution is its simplicity, since it does not require the presence of a slave SIM Toolkit application, as in the case of Method 1.

On the other hand, the drawback of Method 2 is that very few SIM Smart card operating systems fully implement this functionality. In general, an application of a server can send a command script in a short message in order to be executed, but the SIM smart card does not return the result of the command. If, for example, the application implemented in the server needs to know the contents of a file in the SIM smart card, it cannot do so in the majority of SIM smart cards.

#### Calling a function of a library of the SIM smart card

As indicated above, a SIM Toolkit application may need to request the execution of a function included in a library of the SIM smart card (the aforementioned operation c)). There are two main categories of functions in a SIM smart card.

**THIS PAGE BLANK (USPTO)**

1) the functions that use in their parameters at least one secret key stored in the smart card; these functions are used to encrypt, decrypt, sign or verify a signature; and

2) the functions that, on the contrary, do not use secret keys.

Functions in the first category cannot be remoted to a server if it is necessary to maintain a high degree of security, as mentioned above. A slave application 23 (Fig. 3) must be capable of calling them following a request from the master application 30M.

A convention must exist between the slave application 22 and the master application 30M in order to allow the latter to perform encryption/decryption and signature operations with secret keys of the SIM smart card 2.

For example, the master application 30M sends a message to the slave application 22 in which it indicates the nature of the cryptological function to be performed (for example an encryption using the algorithm known as "DES," for "Data Encryption System"). It also indicates the references of the key to be used, stored in the SIM smart card, and the message to be encrypted. The slave application 22 calls the appropriate encryption function and returns the result to the master application 30M.

For the second category of functions, it is possible to use the same method as that used for the first category, but according to an advantageous characteristic of the invention, these functions are implemented directly in a remote server 3. The advantage of this solution is that the processing is done without the need for a connection to a machine that is *a priori* much more powerful than the SIM smart card 2.

According to one of the characteristics of the invention, parts of the SIM Toolkit applications are implemented directly in one or more remote servers 3. To guarantee easy migration of these SIM Toolkit applications from the SIM smart cards, it is also necessary to implement all the associated functions that are located in the libraries of the SIM smart card.

To give an example, in so-called "Java" (registered trademark) cards, these functions are constituted by "Javacard APIs," GSM 03.19 APIs, and so-called "proprietary," i.e. specific APIs. "Java" is an object-oriented programming language developed by Sun Microsystems, Inc., and APIs are programmable interfaces with applications. The Java language specifically makes it possible to develop short

**THIS PAGE BLANK (USPTO)**



applications known as "applets." The SIM Toolkit applications can be created based on applets.

Using these provisions specific to the invention, it is possible to ensure that an application in existing SIM Toolkit technology, which in the prior art is executed in a SIM smart card, can also be executed in a remote server, without its being necessary to modify a line of code, which constitutes an additional advantage of the invention.

It has been assumed up to this point that the so-called short message technology (i.e., in accordance with the GSM 03.40 standard) is used as the transport technology. The use of this technology is advantageous because:

- 1) it is widely use in GSM networks today; and
- 2) it is available in the events and the proactive commands of the SIM Toolkit standard (i.e., in accordance with the GSM 11.14 standard).

However, it should be clear that it is also possible to use other technologies for transport through wireless transmission links that exist between a SIM smart card and a remote server, whether these technologies are currently available or will be in the future.

The mechanisms of the slave and reporter SIM Toolkit applications defined above do not require any modifications, which gives the method according to the invention great perennality.

In the mechanism of the slave and master SIM Toolkit applications, the slave SIM Toolkit application has been assumed to be a complete slave. It is also possible, while remaining within the scope of the invention, to consider slave SIM Toolkit applications that have a certain "intelligence." This type of application, which will be called a "hybrid," is capable both of obeying a master application and of performing local operations autonomously. In essence, a SIM Toolkit application, although it is a slave, continues to have the capabilities inherent in conventional SIM Toolkit applications.

Likewise, it is possible to add a functionality of a similar type, i.e. a certain "intelligence," to the reporter applications.

One is led to conclude that remoting application functionalities from a SIM smart card to a remote server increases the traffic in the network and may, under certain unfavorable conditions, have non-negligible consequences on the response time, since the transfer rate of the short message protocol is low.

**THIS PAGE BLANK (USPTO)**

Hence, in practice, the SIM Toolkit applications most often preferred are both slave and autonomous, and/or are both reporter and autonomous, which makes it possible to minimize the negative impact of the aforementioned increase in traffic.

In an equally practical way, a compromise is sought between the use of the resources of the SIM smart card and the sending of short messages, which can be detrimental in terms of performance.

It should also be noted that authentications must take place between the SIM Toolkit applications implemented in the SIM smart card, whether they be slave or reporter, and the applications implemented directly in a server. They can be performed in compliance with the GSM 03.48 standard.

This standard also provides for the encryption of certain information that is transported during exchanges between a SIM smart card and a remote server.

In general, a master application must communicate with several slave applications. To do this, it is advantageous to use the so-called "Threads" technique when the APIs are implemented in the servers.

In the current state of the art, SIM smart cards of the aforementioned Java type, which implement the GSM 03.19 standard, are unable to send a command to the mobile equipment without passing through an object class known by the name "sim.toolkit.ProactiveHandler". When a slave SIM Toolkit application receives a proactive command sent by a master application, it must reconstruct it using methods of an object class known by the name "ProactiveHandler". It is clear that it is therefore necessary to redo all the work prepared by the server that sent the command, before sending a proactive command to the mobile equipment.

In order for the mechanism of the slave and master applications to retain all of its advantages according to one of the characteristics of the invention, there is a function is advantageously implemented in the SIM smart card that does nothing more than send the mobile equipment a proactive command from any byte array. The slave SIM Toolkit application can then accept the proactive command received, which command was prepared and sent by the master application. It then sends it to the mobile equipment without performing any additional operation.

#### Practical exemplary embodiment

We will now describe in greater detail a practical exemplary embodiment in reference to Figs. 4 and 5.

**THIS PAGE BLANK (USPTO)**

It is assumed that it is necessary to access  $n$  services implemented in a short message server. Hereinafter, these services will arbitrarily be called *Service 1*, *Service 2*, ..., *Service n*. It is assumed that the SIM Toolkit applications are created based on Java applets.

The development of such an application with conventional SIM Toolkit technology, i.e. according to the prior art, requires the development of:

- 1) a SIM Toolkit application that may be called "*AppST*", implemented in a SIM smart card; and
- 2) another application that may be called "*AppOTA*", implemented in a remote server that will be called "*OTA*" (for "*Over the Air*").

The application "*AppST*" responds to two events, which are: "*Menu Selection*" and "*SMS PP Download*".

When the application "*AppST*" receives the event "*Menu Selection*", it sends the mobile equipment a proactive command called "*Select Item*", i.e. the selection of an item on the menu (a service) from among the  $n$  services proposed.

The user chooses, for example, the service with the rank or arbitrary subscript  $i$ , or *Service i*. An applet of the application "*AppST*" sends, in a proactive command, a short message to the application "*AppOTA*", indicating to it that the user is requesting the service *Service i*.

The application "*AppOTA*" receives the short message coming from the application "*AppST*" and responds to it by returning it the content of *Service i* in another short message.

When the application "*AppST*" receives the short message coming from the application "*AppOTA*", it sends a proactive command of the type called "*Display Text*" in order to display its content on the screen of the mobile equipment.

Fig. 4 is a diagram that schematically illustrates the preceding eight steps according to the prior art:

- Step 1: the sending by the circuits 10 of the mobile equipment 1 of "*Menu Selection Event*" to the application "*AppST*" 30';
- Step 2: the sending by the application "*AppST*" 30' of "*Select Item*" to the circuits 10 of the mobile equipment 1;
- Step 3: the response from these circuits by sending "*Terminal response*" to the application "*AppST*" 30';

**THIS PAGE BLANK (USPTO)**

- Step 4: the sending by the latter of "*Send SM (subscript i)*" (send short message with subscript *i*) to the application "*AppST*" 30';
- Step 5: the sending by the latter of "*Short Msg (subscript i)*" (sending of the short message with subscript *i*) to the application "*AppOTA*" 21';
- Step 6: the response from the latter and sending of "*Short Msg (Service 'i')*" (short message for the service with subscript "*i*");
- Step 7: the sending by the circuits 10 of the mobile equipment 1 of "*SMS PP Download Event*" to the application "*AppST*" 30'; and
- Step 8: the sending by the application "*AppST*" 30' of "*Display Text (Service 'i')*" to the circuits 10 of the mobile equipment 1 in order to display the content of the short message associated with the service with the subscript "*i*" so as to display the content on a screen 11 of the mobile equipment 1.

The development of this same application according to the method of the invention takes place as described below, in reference to Fig. 5

Two SIM Toolkit applications constituted by Java applets are installed in the smart card 2: the first is the reporter application 21, which transmits the events received in short messages to a corresponding application, or master application 30M, of the server 3.

The second is the slave application 22, which executes the orders from the master application 30M of the server 3.

It should be noted that the master application 30M of the server 3 plays the role of the two applications "*AppST*" and "*AppOTA*" of the prior art described in reference to Fig. 4.

Once this application 30M receives the event "*Menu Selection*", it becomes the master of the slave SIM Toolkit application 22.

It first asks it to transmit to the circuits 10 of the mobile equipment 1 the aforementioned proactive command "*Select Item*". When it receives the response to this command, it again asks it to execute the proactive command "*Display Text*" in order to display the service selected.

The method according to the invention, for the application described, then includes the twelve steps detailed below:

**THIS PAGE BLANK (USPTO)**



- Step 1: the sending by the circuits 10 of the mobile equipment 1 of "*Menu Selection Event*" to the reporter application (this step is initiated by the user of the mobile equipment 1);
- Step 2: the response and sending by the reporter application 21 of "*Send SM (Menu Selection)*" (send a short menu selection message) to the circuits 10 of the mobile equipment 1;
- Step 3: the sending by the circuits 10 of the mobile equipment 1 of "*SM (Menu Selection)*" to the application 30M (the "*AppST*" part of this application);
- Step 4: the processing and sending by the application 30M of "*SM(Select Item)*" to the circuits 10 of the mobile equipment 1;
- Etape 5 : the sending by the latter of "*SMS PP Download Event*" to the slave application 22;
- Step 6: the processing by the slave application 22 and sending of "*Select Item*" to the circuits 10 of the mobile equipment 1;
- Step 7: the sending by the circuits 10 of the mobile equipment 1 of "*Terminal Response (subscript i)*" to the slave application 22;
- Step 8: the sending by the latter of "*Send SM (Subscript 'i')*" to the circuits 10 of the mobile equipment 1;
- Step 9: the sending by the circuits 10 of the mobile equipment of "*SM (selected subscript 'i')*" (short message for processing with the selected subscript "i") to the application 30M (the "*AppOTA*" part);
- Step 10: the processing and sending by the application 30M of "*SM(Display Text Service 'i')*" to the circuits 10 of the mobile equipment 1;
- Step 11: the sending by the latter of "*SMS PP Download Event*" to the slave application 22; and
- Step 12: the processing and sending of "*Display text (Service 'i')*" to the circuits 10 of the mobile equipment 1, in order to display the content of the short message.

The implementation of the method according to the invention causes a slight increase in traffic in the network, since the number of steps is greater for the same application. However, the main application associated with a given service has been remotored from the SIM smart card 2 to the server 3. It follows that the number of services is potentially no longer limited, since it is no longer necessary to load so

**THIS PAGE BLANK (USPTO)**

many applets into the SIM smart card 2. The memory resources of the server 3 are in fact incomparably greater than those present in the SIM smart card 2. Likewise, the processing speed is higher, since the processor or processors present in the server 3 are also much more powerful than those that can be installed in the SIM smart card 2.

Furthermore, depending on the precise context in which he is working, a developer of software applications retains the capability to distribute the operations to be performed in an optimized way between the SIM smart card 2 and the server 3, according to an additional advantageous aspect of the invention that has been explained.

To do this, certain SIM Toolkit applications can be left in the SIM smart card 2. These applications work in a way identical, or at least very similar, to the applications of the prior art.

According to another variant of embodiment permitted by the method of the invention, all or part of the slave 22 and/or reporter 21 applications can be of the aforementioned hybrid type, i.e., they can retain a certain autonomy. It follows that, in this case, some of the operations continue to be performed locally, which proportionally reduces the traffic between the SIM smart card 2 and the remote server(s) 3.

Through the reading of the above, it is easy to see that the invention achieves the stated objects.

In particular, it makes it possible to remote "intensive" operations that use a lot of computer resources to data processing systems (remote servers) that have no limitations, or at least no substantial limitations, particularly in terms of data storage. Moreover, the operations can be performed at high speed, since the computing means present in these system are also very fast and powerful.

According to another aspect of the invention, although the method according to the invention may entail excess traffic under certain conditions, this drawback can be greatly minimized by optimizing the part of the operations that is remoted and the part of the operations that is still performed locally, i.e. in the SIM smart card or any module functioning as such.

Because of this, the invention makes it possible to offer a virtually unlimited number of services without having to accordingly increase the quantity of data to be stored in the SIM smart card, or at least while increasing it only marginally.

**THIS PAGE BLANK (USPTO)**

It should also be understood that the aforementioned remoted applications include SIM Toolkit applications *per se*, but also associated data files. For example, it may be advantageous to remote a user's personal data, which is normally called his "environment," to a remote server: address book, list of telephone numbers, etc. Here again, the size of these files becomes virtually unlimited.

Finally, it may be said that the invention offers the advantage, when an update of one or more application(s) must be performed, if the latter is/(are) installed in a remote server, that this update can be performed by the operator in a way that is very simple and fast, since it is centralized. In the case of SIM Toolkit applications that are standard, i.e. according to the prior art, installed in smart cards, the same operation would require the modification of all of the smart cards storing the applications to be updated, i.e. most often their replacement.

It should be clear, however, that the invention is not limited to just the exemplary embodiments explicitly described, particularly in connection with Figs. 1 through 3 and 5.

Moreover, as indicated, it is not limited to just the transmission protocols that use short messages.

Finally, while it advantageously applies to telephone networks using the GSM standard, other standards may be suitable, particularly the standards currently under development: "GPRS", "UTMS", etc. Generally, the invention is applicable each time a unit of mobile equipment is used with a smart card or any similar embedded system, and whenever there is a separation between functions installed directly in this embedded system and functions present in the mobile equipment.

It also makes it possible to interface with applications of the WAP type or to perform functions of this type. For example, a master application present in a remote server can directly access the Internet at the request of the mobile equipment, without first passing back through the mobile equipment. The result of the requests made is then sent to the slave application, according to the method specific to the invention.

**THIS PAGE BLANK (USPTO)**

CLAIMS

1. Method for transmitting and processing digital data in a mobile telephone network, said network comprising at least one unit of mobile equipment and a remote server comprising information processing and data storage means communicating with one another via said mobile telephone network, said mobile equipment cooperating with an embedded microchip system comprising information processing and data storage means for storing at least certain pieces of software capable both of controlling said mobile equipment by sending given commands and of reacting to events originating from this equipment by executing instructions associated with said events, in order to perform functionalities associated with at least one predetermined application, characterized in that it includes the implementation of at least a first particular piece of software (21) of a so-called reporter type, stored in said data storage means of said embedded microchip system (2 – 20), and the implementation of at least one associated piece of software (30M) stored in said data storage means of one of said remote servers (3), in that said piece of software of the reporter type (21) retransmits to said associated piece of software (30M) data characteristic of said events received from said mobile equipment (1 – 10) and in that said associated piece of software (30M) executes, using said information processing means of said remote server (3), upon reception of said characteristic data, all or some of said instructions associated with one of said predetermined applications, and retransmits results of said execution to said mobile equipment (1 – 10) and/or to said embedded microchip system (2 – 20).

2. Method according to claim 1, characterized in that, said embedded microchip system (2 – 20) being under the control of a given operating system, said associated piece of software (30M) implemented in one of said remote servers (3) transmits said execution results in the form of commands sent directly to said operating system in order to perform a given operation and in that results of this operation are retransmitted to said associated piece of software (30M).

**THIS PAGE BLANK (USPTO)**



3. Method according to claim 1, characterized in that, said associated pieces of software (30*M*) implemented in said remote servers (3) being of a so-called master type, it includes the implementation of at least one second particular piece of software (22) of a so-called slave type, stored in said storage means of said embedded microchip system (2 – 20), in that each of said pieces of software of the slave type (22) receives commands from one of said pieces of software of the master type (30*M*) that is associated with it, and executes said commands using said information processing means of said embedded microchip system (2 - 20), and in that said piece of software of the slave type (22) retransmits results of said execution of commands to said associated piece of software of the master type (30*M*).

4. Method according to claim 3, characterized in that said pieces of software of the reporter (21) and/or slave (22) types are associated with an additional functionality of a so-called autonomous type, so that these pieces of software (21, 22) can execute directly in said embedded microchip system (2 – 20) a pre-established part of said predetermined applications.

5. Method according to claim 4, characterized in that said mobile telephone network complies with the standard known as GSM and said pieces of software comply with the GSM 11.14 standard.

6. Method according to claim 1, characterized in that, said telephone network comprising at least two distinct transmission channels, a so-called voice data channel and a so-called message channel, said transmitted digital data is constituted by messages of a so-called short type comprising 140 octets or 160 septets transmitted through this message channel.

7. Embedded system equipped with a microchip comprising information processing and data storage means for storing at least certain pieces of software capable both of controlling said mobile equipment by sending given commands and of reacting to events originating from this equipment by executing instructions associated with said events, in order to perform functionalities

**THIS PAGE BLANK (USPTO)**

associated with at least one predetermined application, said embedded microchip system cooperating with a unit of mobile equipment linked to a mobile telephone network, said mobile telephone network being connected with at least one remote server comprising information processing and data storage means communicating with said mobile equipment via said mobile telephone network, characterized in that said embedded microchip system (2 -20) stores in its said data storage means at least a first particular piece of software (21) of a so-called reporter type, designed to retransmit to an associated piece of software (30M) stored in said data storage means of one of said remote servers (3) that is associated with it, data characteristic of said events received from said mobile equipment (1 – 10 ), so that said associated piece of software (30M) executes, using said information processing means of said remote server (3), upon reception of said characteristic data, all or some of said instructions associated with one of said predetermined applications, and to retransmit results of said execution to said mobile equipment (1 – 10) and/or to said embedded microchip system (2 – 20).

8. Embedded microchip system according to claim 7, characterized in that, said associated pieces of software (30M) implemented in said remote servers (3) being of a so-called master type, it stores in its said data storage means at least one second particular piece of software (22) of a so-called slave type, designed to receive commands from one of said pieces of software of the master type (30M) that is associated with it, to execute said commands using said information processing means of said embedded microchip system (2 – 20) and to retransmit results of said execution of commands to said associated piece of software of the master type (30M).

9. Embedded microchip system according to claim 8, characterized in that said pieces of software of the reporter (21) and/or slave (22) types are associated with an additional, so-called autonomous functionality, so that these pieces of software can execute directly in said embedded microchip system (2 – 20) a pre-established part of said predetermined applications.

**THIS PAGE BLANK (USPTO)**

## **Pages prior to amendment**

10. Embedded microchip system characterized in that it is constituted by a smart card of the so-called SIM type (2).

**THIS PAGE BLANK (USPTO)**

**FIG. 1**

Serveur – Server

Application du serveur – Application of the server

Equipement mobile – Mobile equipment

Carte à puce "SIM" – SIM smart card

Application "Sim Toolkit" rapporteuse – Reporter SIM Toolkit application

Circuits carte "SIM" – SIM card circuits

Circuits Equipement mobile – Mobile equipment circuits

**FIG. 2**

Application du Serveur Maître – Master Application of the Server

Application "Sim Toolkit" esclave – Slave SIM Toolkit application

(for other terms: see Fig. 1)

**FIG. 3**

(see Figs. 1 and 2)

**FIG. 4**

ART ANTERIEUR – PRIOR ART

Application Serveur – Server Application

Etapes – Steps

(indice i) – (subscript i)

Ecran – Screen

Carte à puce – Smart card

Application "Sim Toolkit" – SIM Toolkit application

(for other terms: see Figs. 1 and 2)

**FIG. 5**

(see Figs. 1 through 4)

**THIS PAGE BLANK (USPTO)**



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**